NORTHERN ARIZONA UNIVERSITY

INF639: Nanoelectronics for Cybersecurity

Section 4: Smart cards & secure elements

Dr. Bertrand Cambou
Professor of Practice NAU, Cybersecurity
School of Informatics, Computing, and Cyber-Systems
Bertrand.cambou@nau.edu

NORTHERN ARIZONA UNIVERSITY

INF 639: Nanoelectronics for cybersecurity

1. From Micro to Nano-electronics
2. Introduction to cryptography
3. Public Key Infrastructure
4. Smartcards
5. Attacks on smartcards
6. MOS transistor & logic circuits
7. Biometry
8. Physical Unclonable Functions (PUF)
9. Access control and authentication
10. Flash Memory devices & security
11. Resistive RAM & security
12. Public key cryptography with PUFs
13. Sensor devices & security
14. Ternary cryptography

NORTHERN ARIZONA UNIVERSITY

4 Smartcards and Secure elements

- 1 General description
  - Why smartcards?
  - Microprocessor cards with crypto-processor
  - Contactless and combi cards
- 2 Security services
  - Cryptographic services, principles, and algorithms
- 3 Software
  - Operating systems
  - Javacard

History and Development

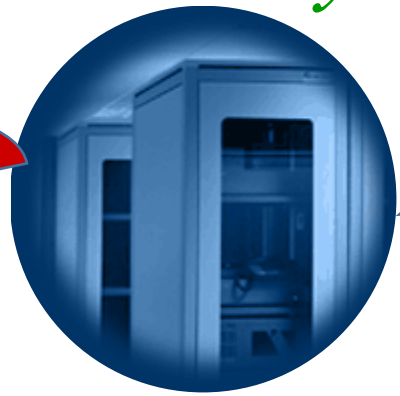
- The Invention of the Smart Card
  - Roland Moreno, in 1974.
  - Innovatron company (Bull, Philips and Schlumberger).
  - public telephone payment system(1983)
  - French standards(1984)
- Development of the technology
  - Contactless in the UK
  - European banks – Europay Master card Visa (EMV)
  - Subscriber Identity Module (SIM) for GSM
  - Access and transport (Myfare)
- Secure elements
  - Crypto-processor for the internet of things
  - Total volume in 2018: 10 Billions
  - Cost between 5 cents and $2

Smart Card Systems

Smart Card

Card Personalization Issuance

Back-end Systems



Post-Issuance Transactions

Accepting Devices

Post-Issuance Transactions

Smart card applications

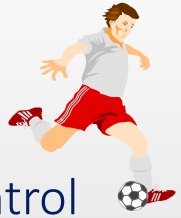
❑Healthcare

- ❑Insurance data
- ❑Personal data
- ❑Personal file

❑Government

- ❑Identification
- ❑Passport
- ❑Driving license

❑ Entertainment



- ❑ Pay-TV
- ❑ Public event access control

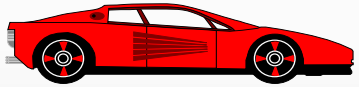
❑Office

- ❑Physical access
- ❑Network access
- ❑Time registration
- ❑Secure e-mail & Web applications

❑Communication

- ❑GSM
- ❑Payphones

❑Transportation



- ❑Public Traffic
- ❑Parking
- ❑Road Regulation (ERP)
- ❑Car Protection VIN No

❑Educational facilities

- ❑Physical access
- ❑Network access
- ❑Personal data (results)
- ❑Copiers, vending machines, restaurants, ...

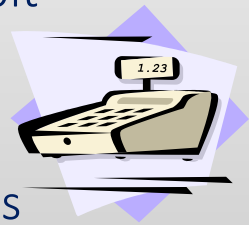
❑E-commerce

- ❑sale of information
- ❑sale of products
- ❑sale of tickets, reservations

❑E-banking

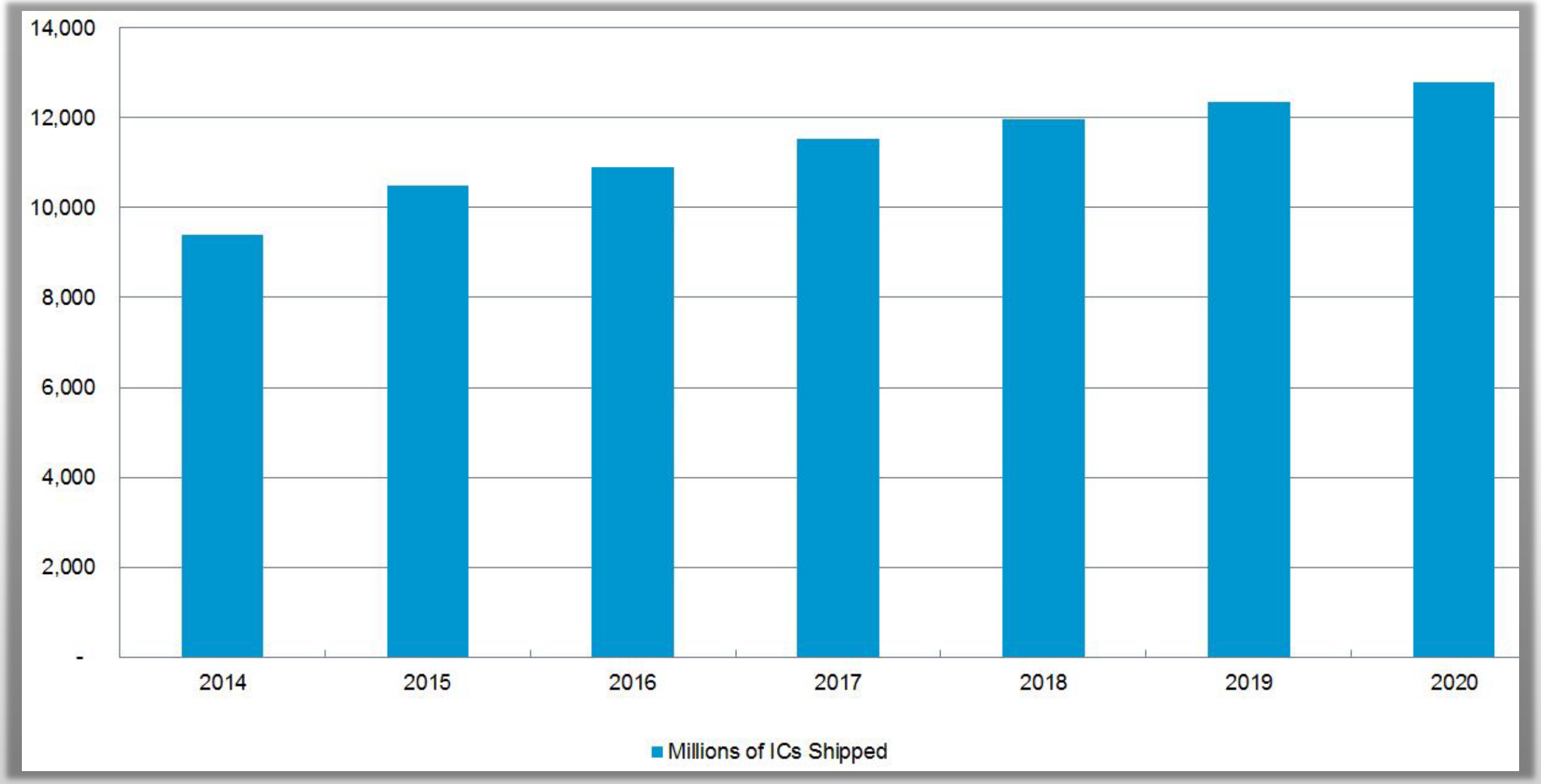
- ❑access to accounts
- ❑to do transactions
- ❑shares

❑Retail

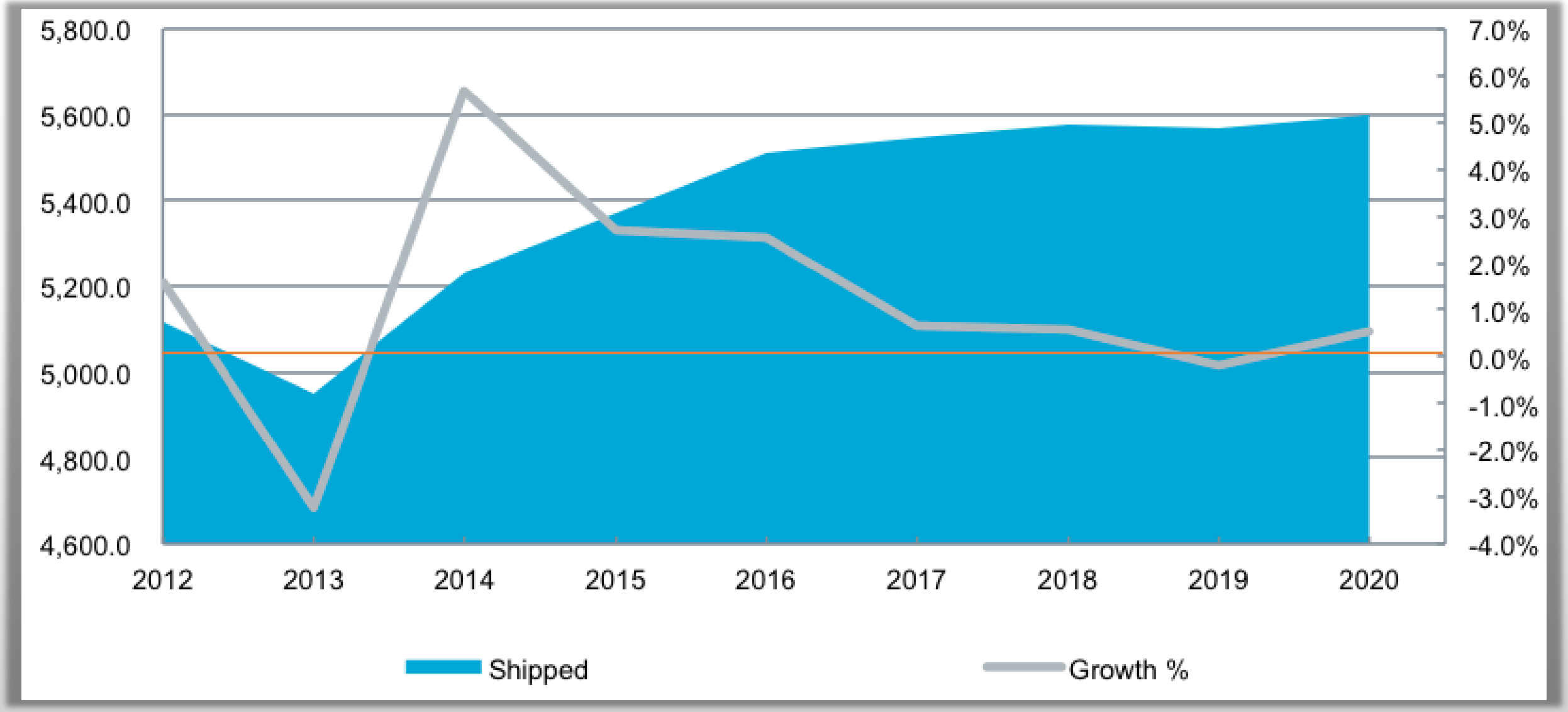


- ❑Sale of goods: Electronic Purses, Credit/Debit
- ❑Vending machines
- ❑Loyalty programs
- ❑Tags & smart labels

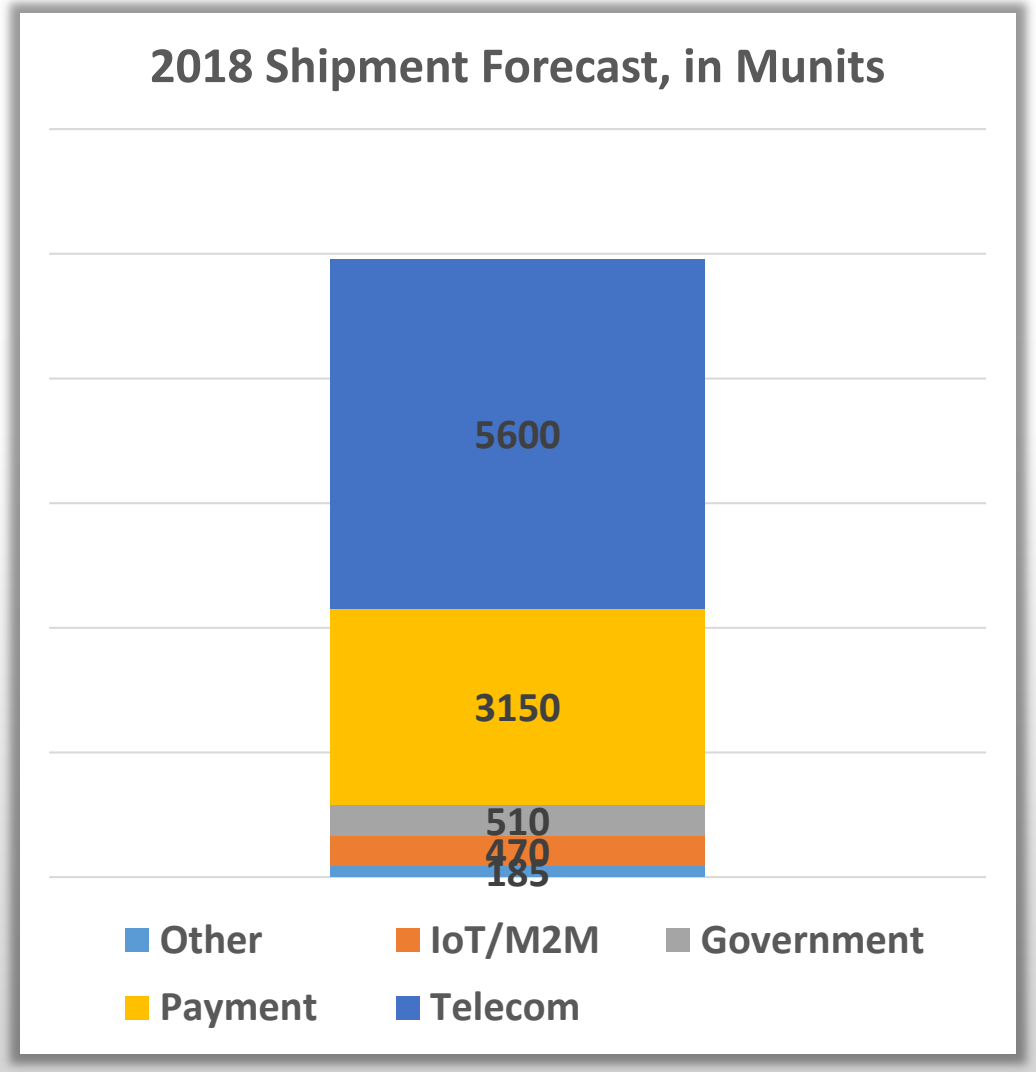
Volume smartcards: world market 2014 to 2020 (Source HIS)

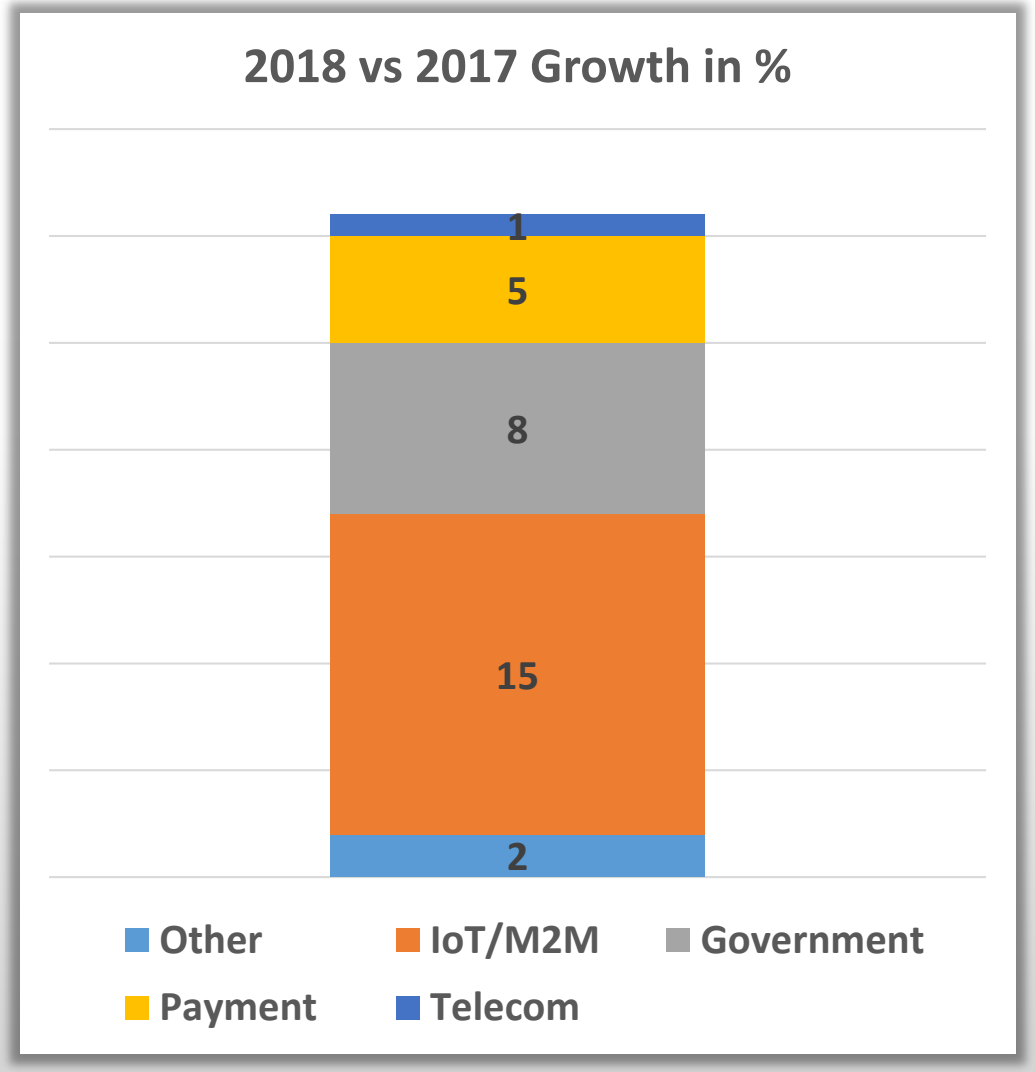


Volume SIM: world market 2014 to 2020 in millions (Source HIS)



Volume smartcards: world market 2014 to 2020 (Source Eurosmart)





Smart Cards Vendor Market Share 2018

1) Idemia: Oberthur + Safran 2)Gemalto acquired by Thales

gemalto security to be free — 30%

OBERTHUR TECHNOLOGIES — 15%

Giesecke & Devrient Creating Confidence. — 15%

SAFRAN Morpho — 10%

东信和平 EASTCOMPEACE

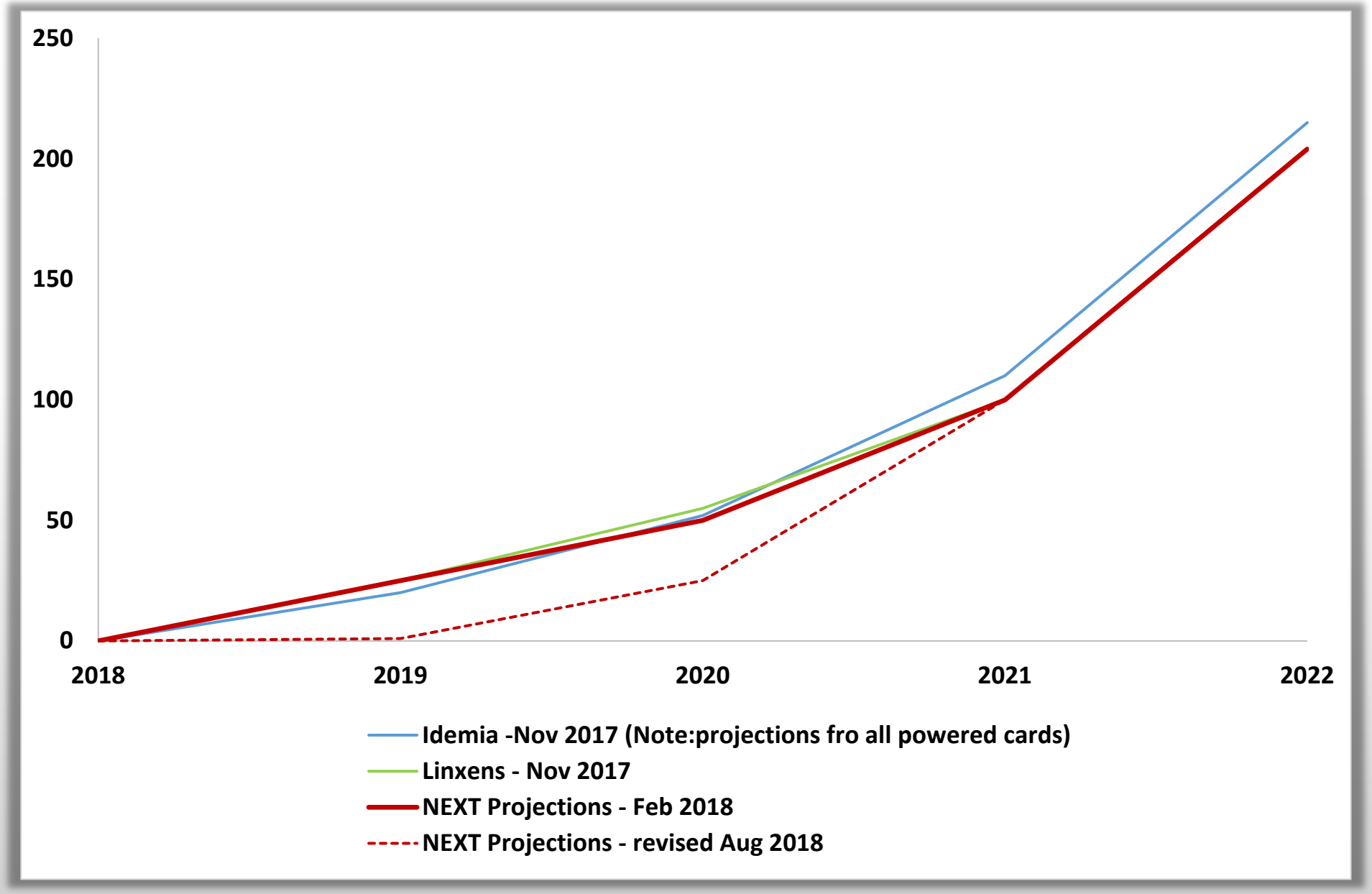
WATCHDATA

30% All others

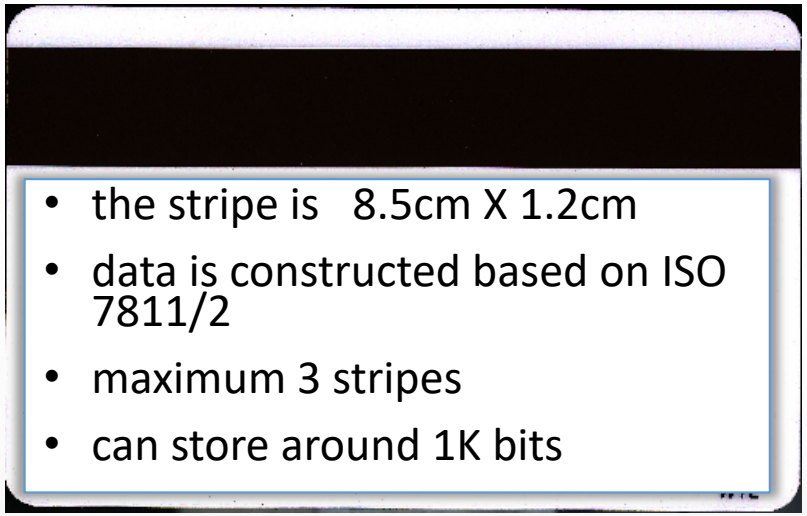
Payment network: world market 2017 (Source Next)

Ranking	Payment Network	Primary issuers	Number of issued cards
#1	VISA	Global	884M*
#2	MasterCard	Global	721M*
#3	Rupay	India	375M
#4	China UnionPay	China, expanding	331M*
#5	AMEX	Global	102M*
#6	JCB	Japan	79M*
#7	Discover	Discover Bank + U.S.	44M

Biometric Smart Card shipments projection in Millions of Units (source NEXT)

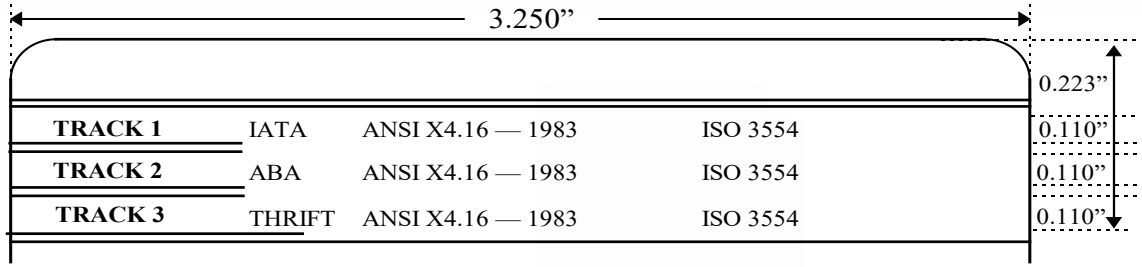


First card system: Magnetic Card



- the stripe is 8.5cm X 1.2cm
- data is constructed based on ISO 7811/2
- maximum 3 stripes
- can store around 1K bits

Track	Record density bits/inch	Capacity
1	210	79 (7 bits/char.)
2	75	40 (5 bits/char.)
3	210	107 (5 bits/char)



Track 1

SS	FC	PAN	FS	NAME	FS	Additional Data	ES	LRC
		Primary Acc. No. (19 digits max.)		Name (26 alphanumeric characters max.)		• Exipiry Date 4 • Restriction or Type 3 • Offset or PVN 5 • Discretionary Data		

SS Start Sentinel % FC Format Code

FS Field Seperator { ES End Sentinel ? LRC Longitudinal Redundany Code

Track 2

SS	FC	PAN	FS	Additional Data	ES	LRC
		Primary Acc. No. (19 digits max.)		• Exipiry Date 4 • Restriction or Type 3 • Offset or PVN 5 • Discretionary Data		

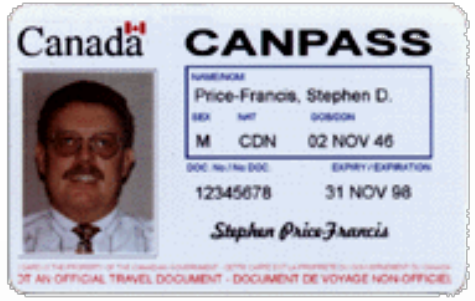
SS Start Sentinel ; FC Format Code

FS Field Seperator = ES End Sentinel ? LRC Longitudinal Redundany Code

Magnetic stripe Content of Financial Cards

Fraud card activities

- ***Stealing*** — A legal card may be stolen and used in ATMs or EPOSs.
- ***Altering and re-embossing*** a genuine card, that is modifying the visual features of card.
- ***Skimming*** or altering the original electronic data stored on the magnetic stripe, for example the expire date or the credit limit.
- ***Buffering*** or re-encoding the original data to the magnetic card. This technique is commonly used in producing card counterfeits of store-value ticket.
- ***Copying*** of data from a genuine card to another in an on-line fashion "white plastic fraud"
- ***Counterfeiting*** — "color plastic fraud" may be prepared by reading another legal card and encoding the same information onto another fraud card in an off-line fashion.



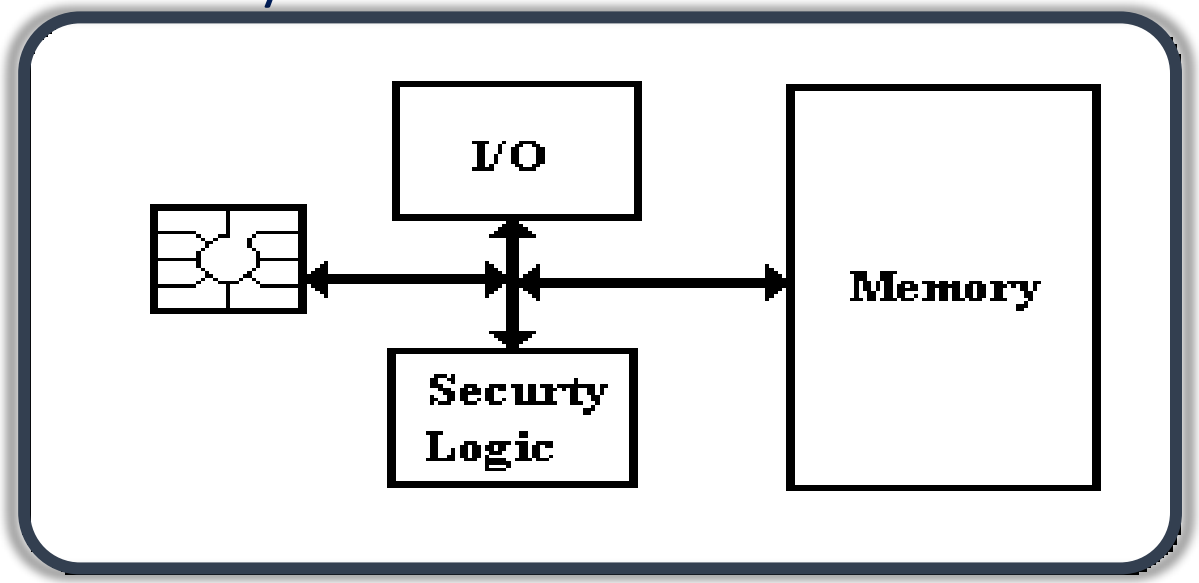
Fraud

Card protection activities

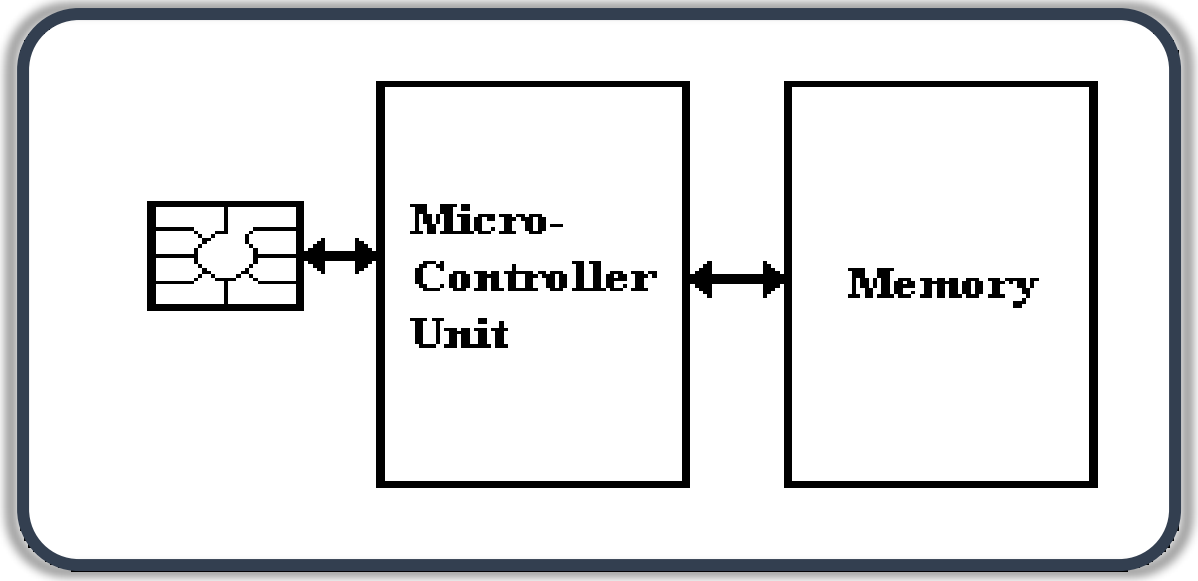
- Visual Protection Technologies
  - Holograms
  - Photocard
  - Embossed Information
  - Ultraviolet Pattern
  - Microprints
- Protection on Access
  - PIN
  - Signature
  - DNA
- Verification by Card Content
  - Protection on Modification
    - PVV
    - CVC
  - Protection on Duplication
    - Magnetic Stripe Protection
      - Xsec
      - Xshield
      - Holomagnetic
      - Valugard
      - Magneprint
      - Sandwich
      - Watermark
    - Smart Card
      - Memory Card
      - µP Card

Types of Smart Card

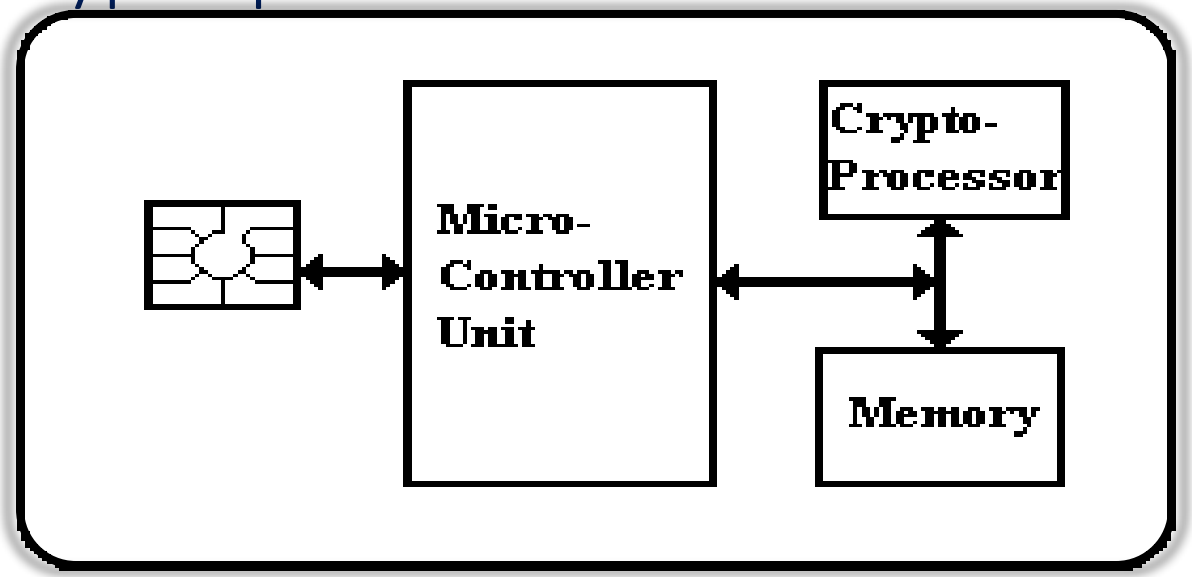
Memory Card



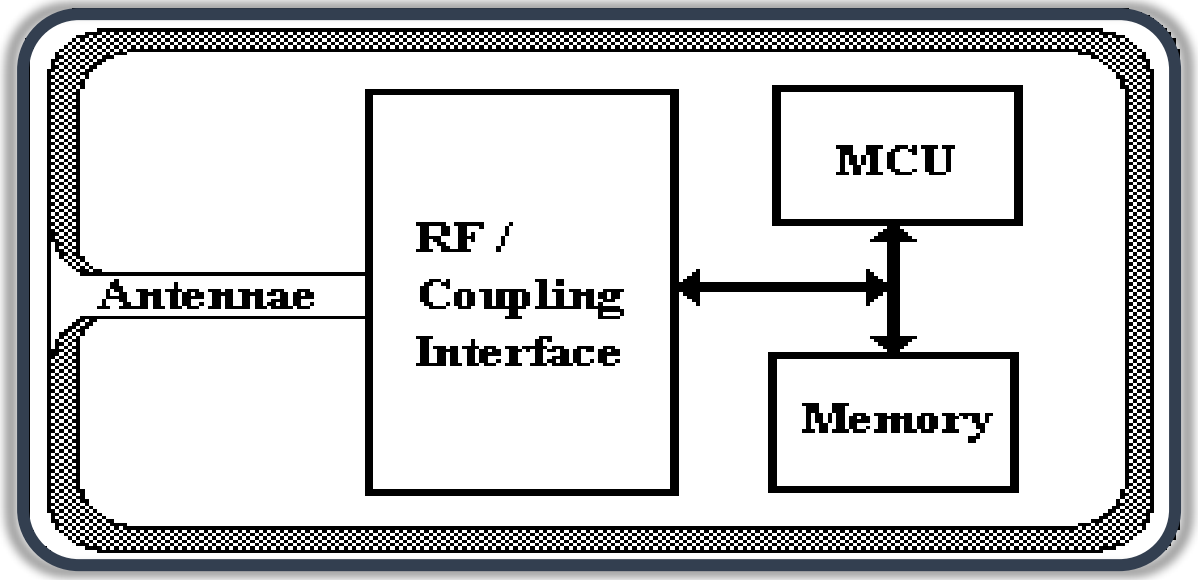
MPU IC card



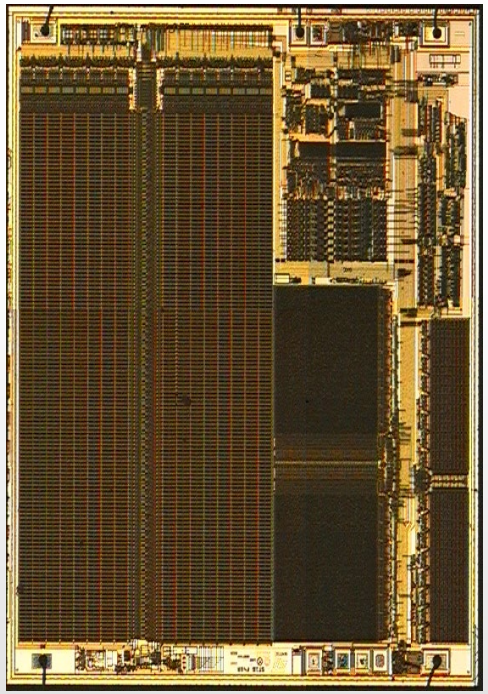
Crypto-processor card

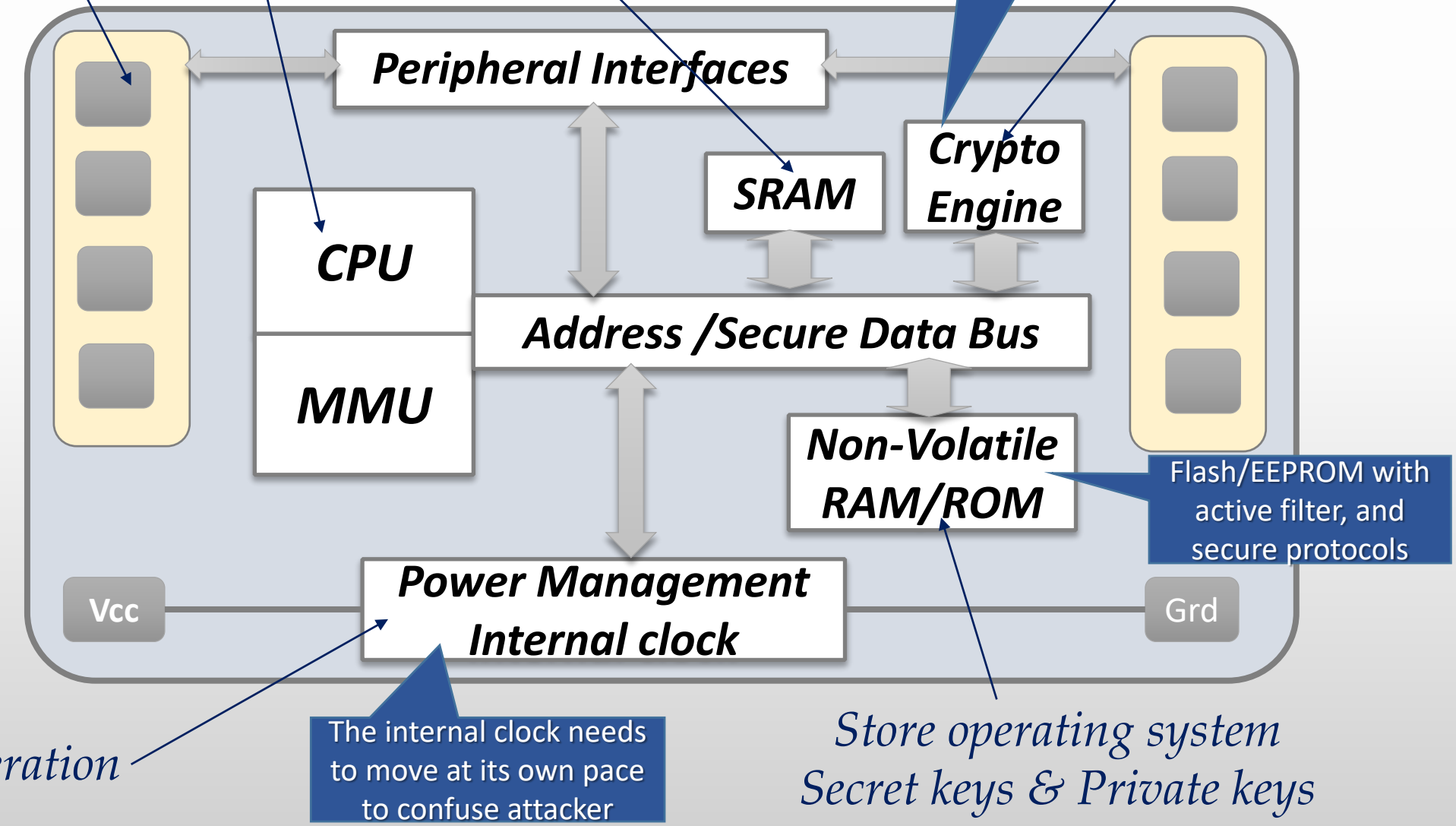


Contactless card



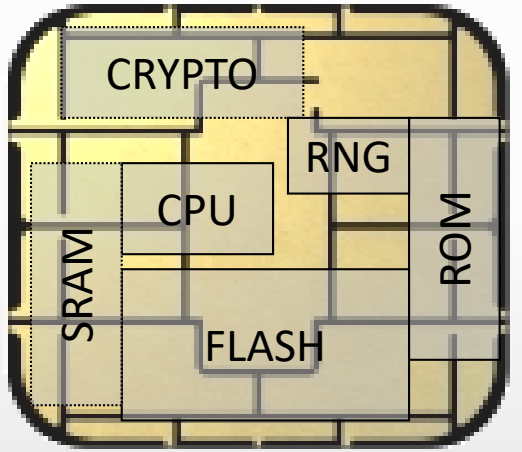
Basic architecture of a secure element

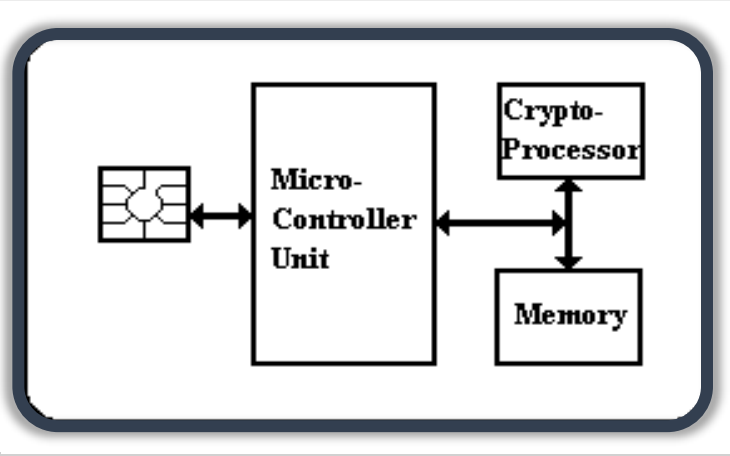




Crypto-processor IC Cards

- Powerful MPU - RISC 16 to 32bit – 50MHz
- Cypto-processor (Ex: Secure core from ARM)
- Secure NV memory (100KB to1MB)
- SRAM (5 to 50KB)
- Store private & secret keys
- Powerful cryptography:
  AES, 3DES, RSA, ECC, SHA2, RNG
- Powerful authentication
- Recognize illegal signal
- Open source OS & API
- Third party application SW





Multi-Application Smart Card

SSL Secure Web

S/Mime Secure Mail

Customer PKI Application

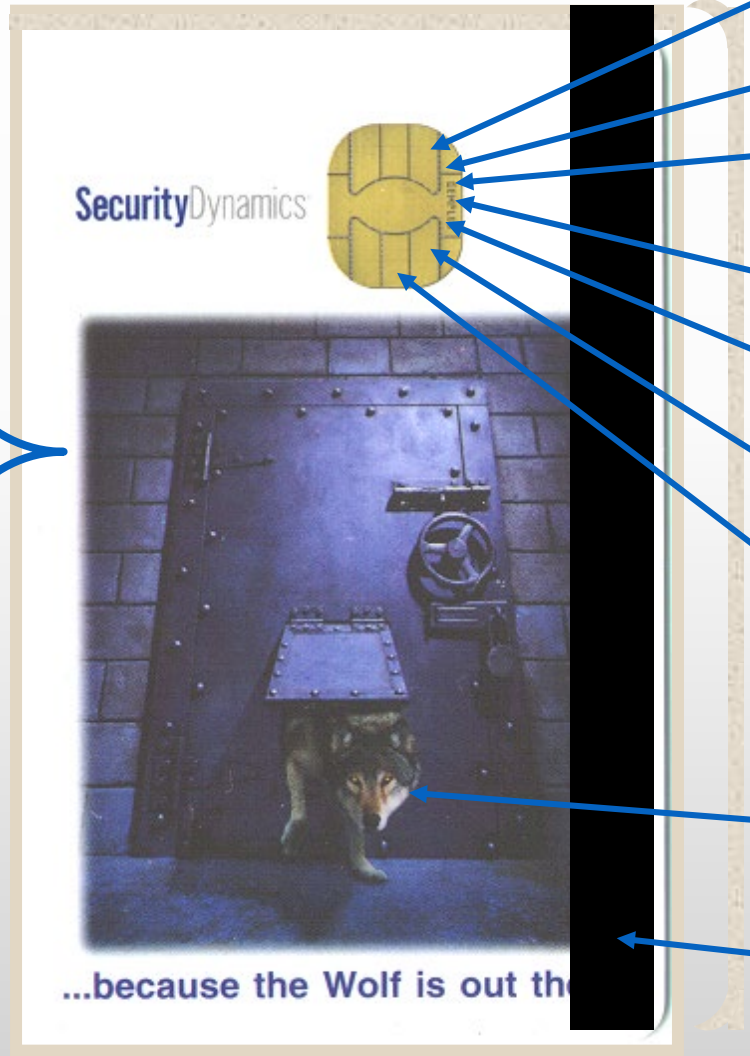
Single Sign-On

Biometric Authentication

Local File Encrypt

Secure Screen Saver

Application Login



Private Key(s)

Digital Certificates

Active Customer Authentication

Biometric Data

Encryption Key

Employee Data

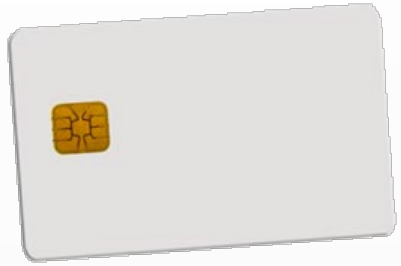
Password Cache

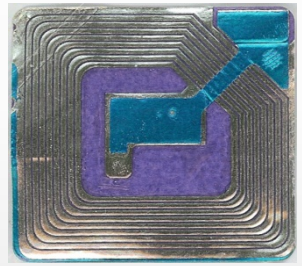
Employee Picture

Magnetic Stripe or RF Door Access

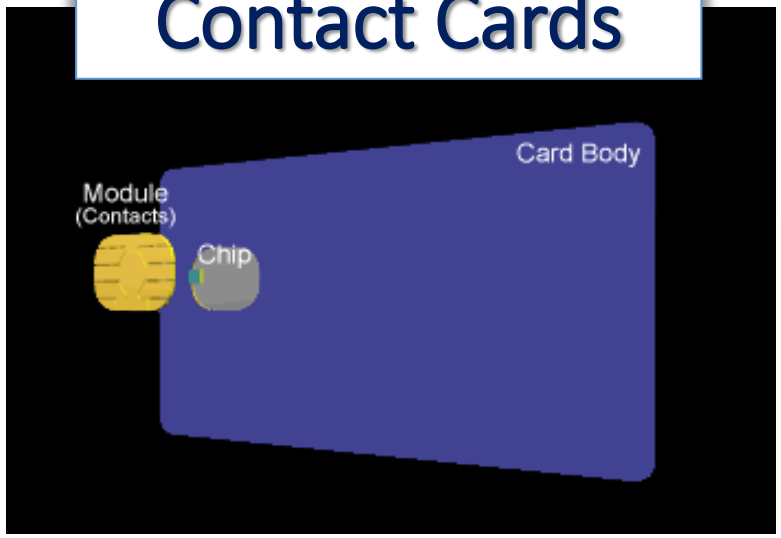
Smart cards forms

- Contact cards (ISO7816-2)
  - I/O data line, voltage and GND line
  - clock line, reset lines
- Contactless cards
  - ISO/IEC 14443 type A/B, radio at 13.56 MHz
  - Chip powered by current induced on antenna by reader
  - Reader → chip communication - relatively easy
  - Chip → reader – dedicated circuits are charged
  - Multiple cards per single reader possible
- Hybrid/combi/dual interface
- Many possible operating systems

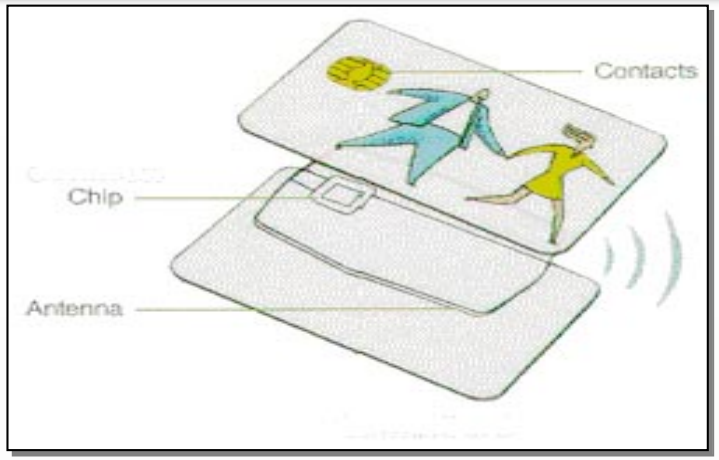




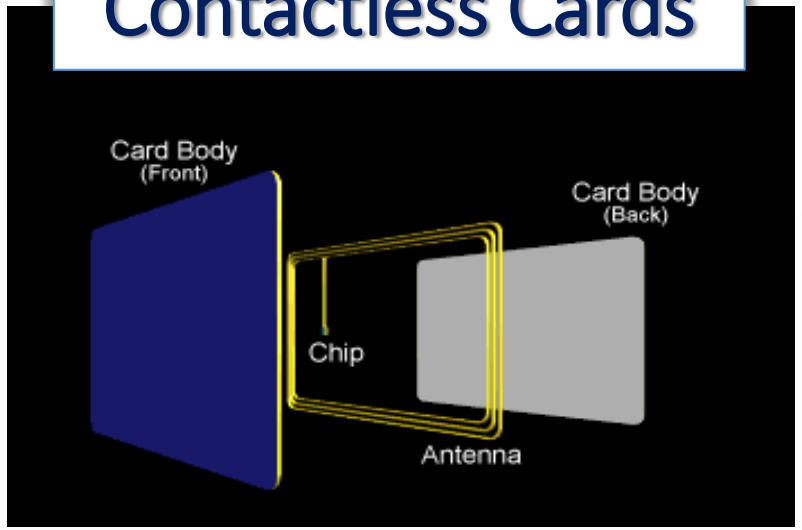
Contact Cards

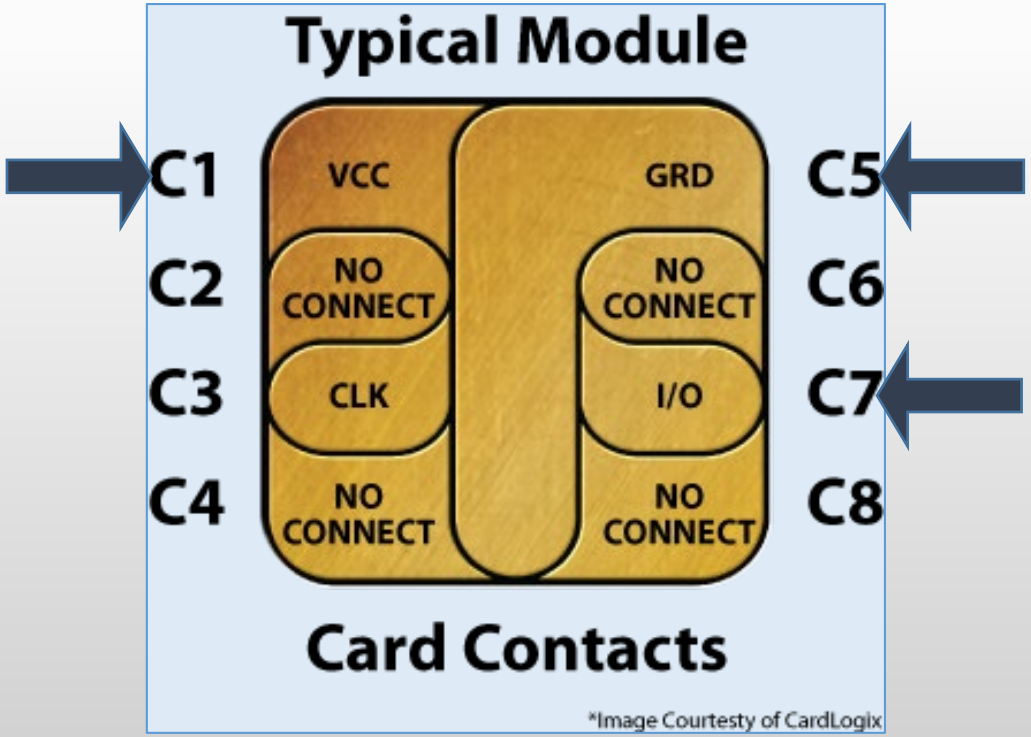


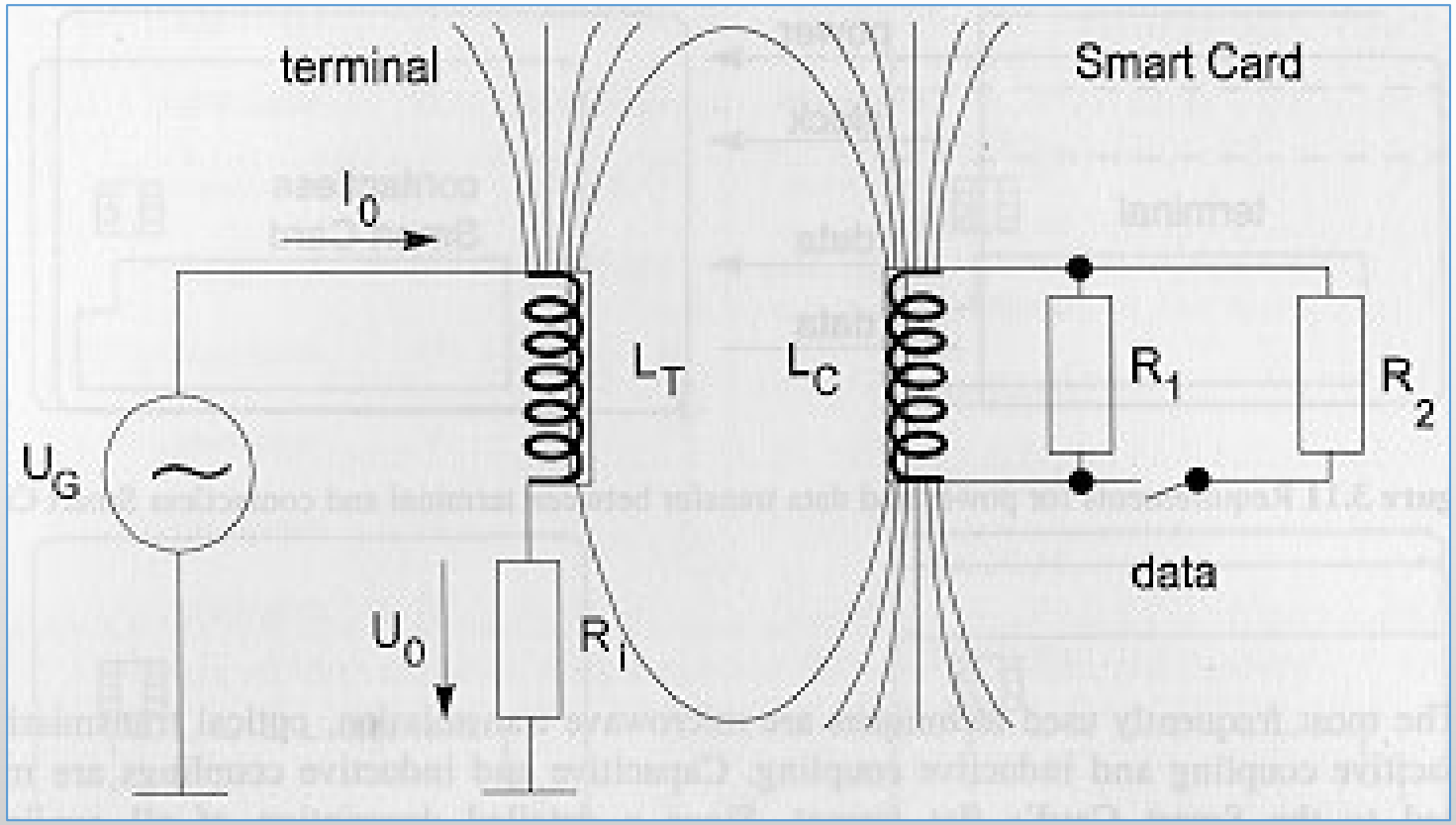
Combi / Hybrid Cards



Contactless Cards

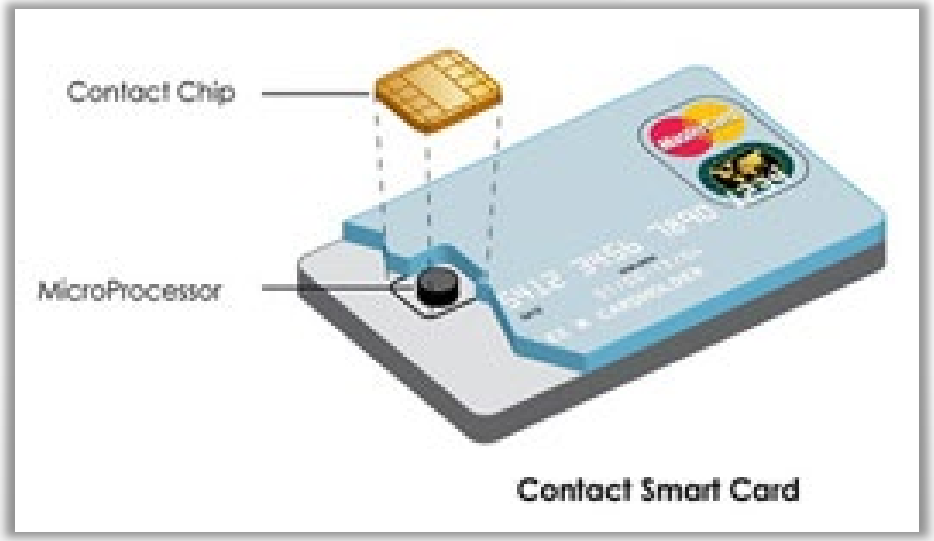




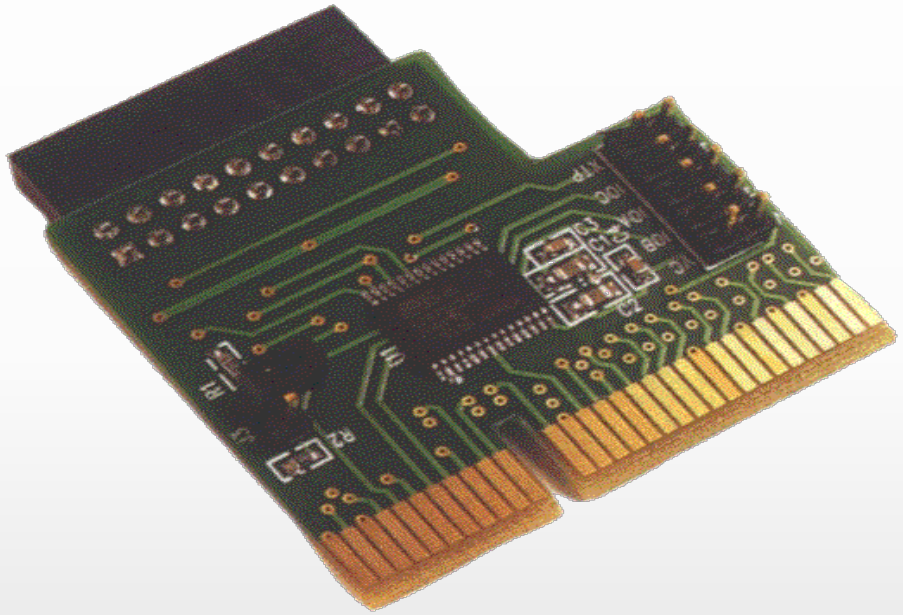


Contact smartcards & Secure Elements

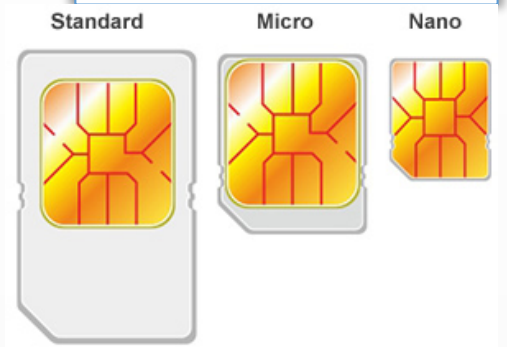
Banking cards

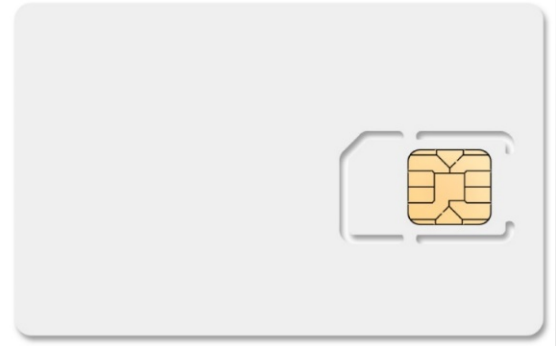


Secure Elements



SIM cards

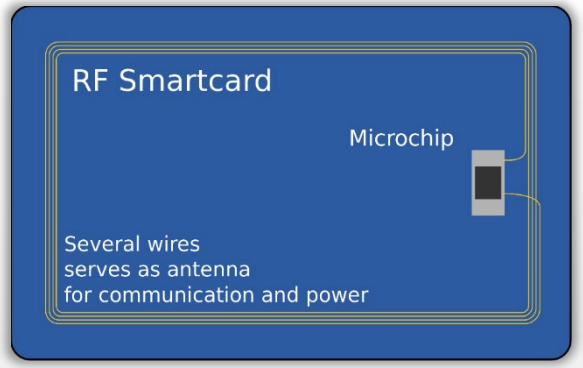




Secure USB

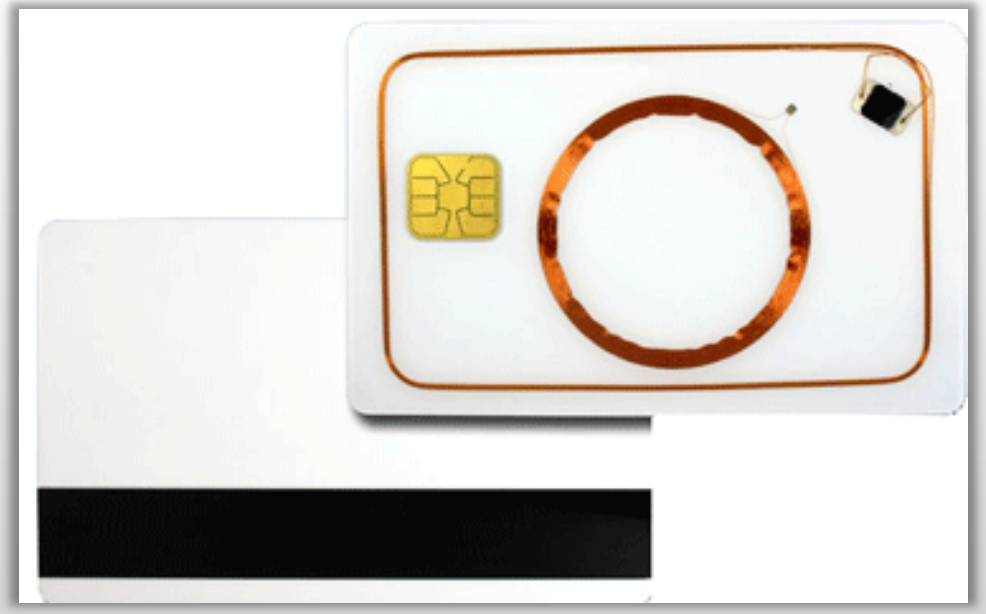
Contactless smartcards

- *Transport*
- *Access*
- *ID cards*



Combi-cards

- *Banks*
- *Fidelity*
- *Retail*



Non traditional form factor

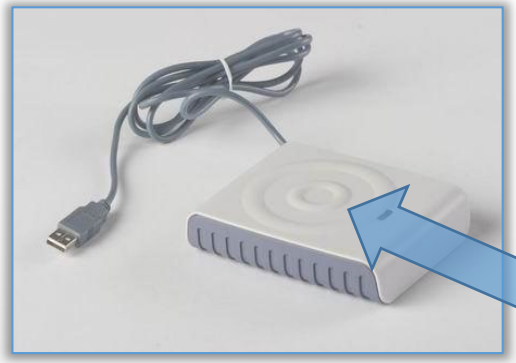
Smart Card Readers

Computer based readers

Connect through USB or COM (Serial) ports

Wireless &NFC readers

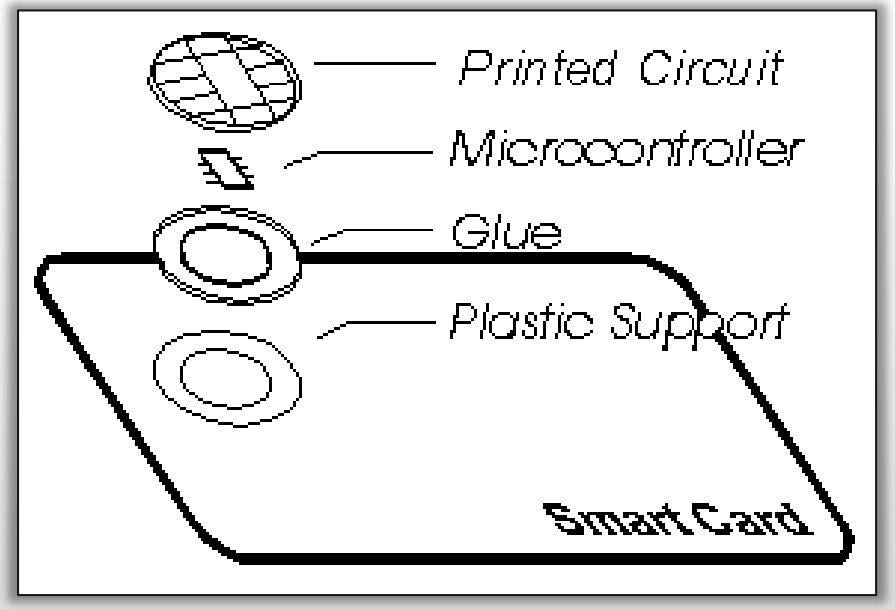
Connect through stabdard wireless protocols such as myfare or NFC

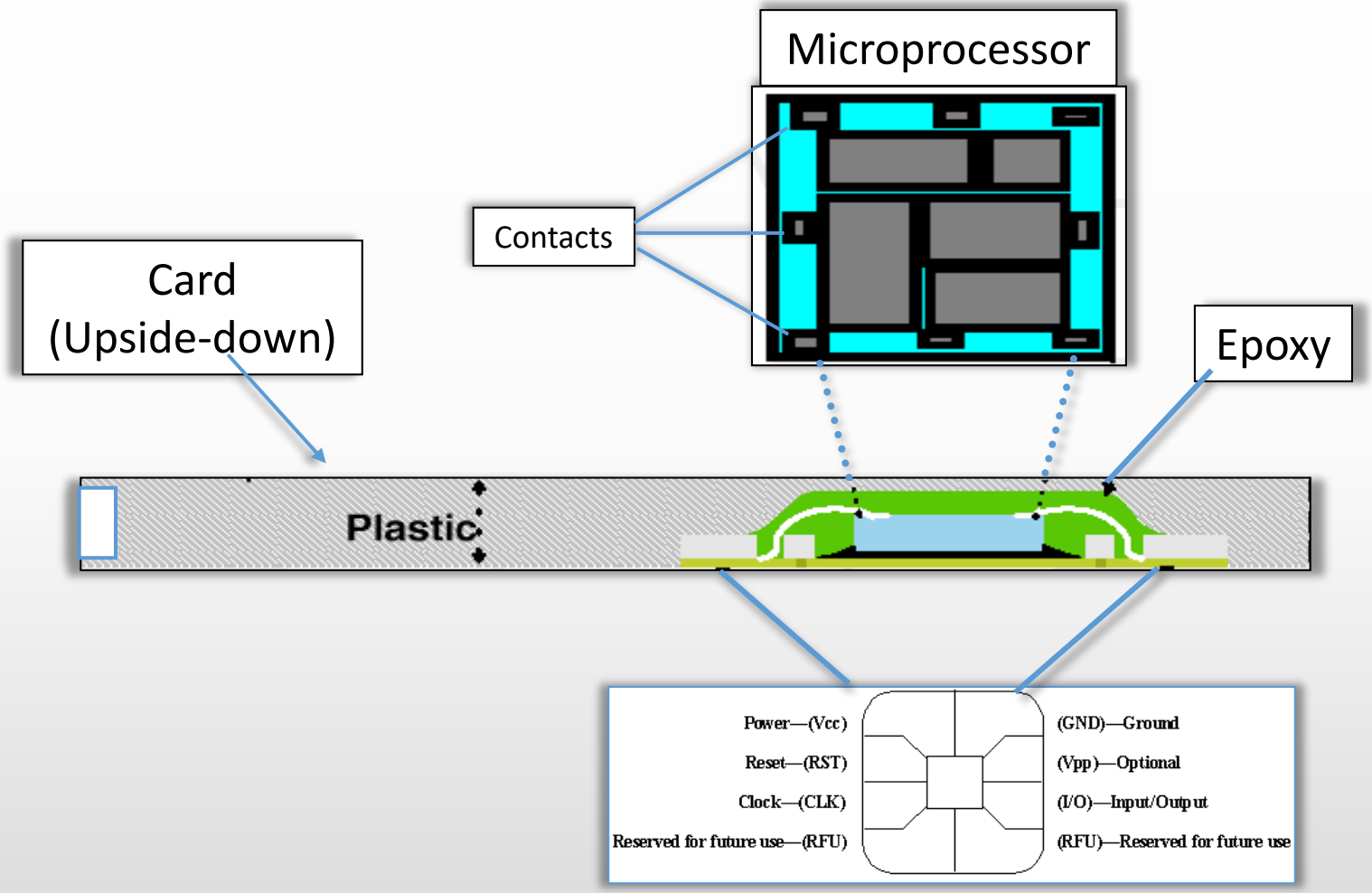


Merchant Payment

Usually with a small screen, keypad, printer, often also have biometric devices such as thumb print scanner.

Physical Structure - ISO 7810/7816





- *Printed circuit provides five connection points for power and data*
- *Chip: Microprocessor & Cryptoprocessor ROM/RAM/NVM*

Infineon: Banking

16-bit CPU
Cryptography
200kByte Flash
6KByte RAM

	Dual-interface & Contactless Security Controller [1]			
Product name	**SLE 77CLFX1367P(M)** SOLID FLASH™	**SLE 77CLFX1567P(M)** SOLID FLASH™	**SLE 77CLFX1847P(M)** SOLID FLASH™	**SLE 77CLFX2007P(M)** SOLID FLASH™
Product description	Dual-interface and Contactless Security Cryptocontroller	Dual-interface and Contactless Security Cryptocontroller	Dual-interface and Contactless Security Cryptocontroller	Dual-interface and Contactless Security Cryptocontroller
Interfaces	ISO 7816, ISO 14443 A/B, ISO 18092 passive mode, Mifare compatible interface, Optimized for sub-ID1	ISO 7816, ISO 14443 A/B, ISO 18092 passive mode, Mifare compatible interface, Optimized for sub-ID1	ISO 7816, ISO 14443 A/B, ISO 18092 passive mode, Mifare compatible interface, Optimized for sub-ID1	ISO 7816, ISO 14443 A/B, ISO 18092 passive mode, Mifare compatible interface, Optimized for sub-ID1
Memory	136kByte SOLID FLASH™, 6kByte RAM	156kByte SOLID FLASH™, 6kByte RAM	184kByte SOLID FLASH™, 6kByte RAM	200kByte SOLID FLASH™, 6kByte RAM
CPU	16-bit	16-bit	16-bit	16-bit
Crypto coprocessor symmetrical	DES, 3DES, AES up to 256-bit	DES, 3DES, AES up to 256-bit	DES, 3DES, AES up to 256-bit	DES, 3DES, AES up to 256-bit
Crypto coprocessor asymmetrical	RSA up to 4096-bit, ECC up to 521-bit	RSA up to 4096-bit, ECC up to 521-bit	RSA up to 4096-bit, ECC up to 521-bit	RSA up to 4096-bit, ECC up to 521-bit
Ambient temperature	-25 to +85°C	-25 to +85°C	-25 to +85°C	-25 to +85°C
Delivery forms	Dual interface module, MCC8, Coil on Module, Wafer sawn	Dual interface module, MCC8, Coil on Module, Wafer sawn	Dual interface module, MCC8, Coil on Module, Wafer sawn	Dual interface module, MCC8, Coil on Module, Wafer sawn
Typical applications	EMV DDA, EMV CDA, Global Platform/Java, Loyalty, ePurse	EMV DDA, EMV CDA, Global Platform/Java, Loyalty, ePurse	EMV DDA, EMV CDA, Global Platform/Java, Loyalty, ePurse	EMV DDA, EMV CDA, Global Platform/Java, Loyalty, ePurse
Certification level	CC EAL5+ high/EMVCo	CC EAL5+ high/EMVCo	CC EAL5+ high/EMVCo	CC EAL5+ high/EMVCo

Infineon: Mobile

32-bit CPU
Cryptography
1.3MByte Flash
32KByte RAM

	SIM & UICCs			
Product name	**SLE 97CNFX1M50PE** NFC Optimized SOLID FLASH™	**SLE 97CUNFX8000PE** SOLID FLASH™	**SLE 97CUNFX1M00PE** SOLID FLASH™	**SLE 97CUNFX1M30PE** SOLID FLASH™
Product description	32-bit SWP SIM-card Security Cryptocontroller	32-bit USB and SWP SIM-card Security Cryptocontroller	32-bit USB and SWP SIM-card Security Cryptocontroller	32-bit USB and SWP SIM-card Security Cryptocontroller
Interfaces	ISO 7816, SWP (Mifare compatible)	ISO 7816, SWP (Mifare compatible), USB	ISO 7816, SWP (Mifare compatible), USB	ISO 7816, SWP (Mifare compatible), USB
Memory	1.5MByte SOLID FLASH™, 32kByte RAM	800kByte SOLID FLASH™, 32kByte RAM	1MByte SOLID FLASH™, 32kByte RAM	1.3MByte SOLID FLASH™, 32kByte RAM
CPU	32-bit	32-bit	32-bit	32-bit
Symmetrical Cryptography	DES, 3DES, AES up to 256-bit	DES, 3DES, AES up to 256-bit	DES, 3DES, AES up to 256-bit	DES, 3DES, AES up to 256-bit
Asymmetrical Cryptography	RSA up to 4096-bit, ECC up to 521-bit	RSA up to 4096-bit, ECC up to 521-bit	RSA up to 4096-bit, ECC up to 521-bit	RSA up to 4096-bit, ECC up to 521-bit
Ambient temperature	-25 to +85°C	-25 to +85°C	-25 to +85°C	-25 to +85°C
Delivery forms	FCOS™ module, VQFN-8, Wirebond module, Chip Scale Package, Wafer sawn	FCOS™ module, VQFN-8, Wirebond module, Chip Scale Package, Wafer sawn	FCOS™ module, VQFN-8, Wirebond module, Chip Scale Package, Wafer sawn	FCOS™ module, VQFN-8, Wirebond module, Chip Scale Package, Wafer sawn
Typical applications	SWP SIM/UICC (NFC), Embedded SIM, CIPURSE™ for mobile	USB SIM/UICC, Embedded SIM	USB SIM/UICC, Embedded SIM	USB SIM/UICC, Embedded SIM
Certification level	CC EAL5+ high/EMVCo	CC EAL5+ high/EMVCo	CC EAL5+ high/EMVCo	CC EAL5+ high/EMVCo

Infineon: Machine to machine

32-bit CPU
Cryptography
600kByte Flash
32KByte RAM
-40°C to 105°C

	Machine-to-Machine (M2M) Cellular			
Product name	**SLM 76CF5120P** SOLID FLASH™	**SLI 76CF3600P** SOLID FLASH™	**SLI 76CF5120P** SOLID FLASH™	**SLM 97CNFX6000PE** SOLID FLASH™
Product description	Security Cryptocontroller optimized for industrial M2M applications	Security Cryptocontroller optimized for automotive M2M applications	Security Cryptocontroller optimized for automotive M2M applications	Security Cryptocontroller optimized for industrial M2M applications
Interfaces	ISO 7816	ISO 7816	ISO 7816	ISO 7816, SWP
Memory	504kByte SOLID FLASH™, 12kByte RAM	360kByte SOLID FLASH™, 8kByte RAM	504kByte SOLID FLASH™, 12kByte RAM	608kByte SOLID FLASH™, 32kByte RAM
CPU	16-bit	16-bit	16-bit	32-bit
Symmetrical Cryptography	3DES, AES up to 256-bit	3DES, AES up to 256-bit	3DES, AES up to 256-bit	3DES, AES up to 256-bit
Asymmetrical Cryptography	–	–	–	RSA up to 4096-bit, ECC up to 521-bit
Ambient temperature	-40 to +105°C	-40 to +105°C	-40 to +105°C	-40 to +105°C
Delivery forms	Wafer sawn, P-M2M4.7, MFF2	MFF2	MFF2	Wafer sawn, P-M2M4.7, MFF2
Typical applications	Industrial M2M, Consumer M2M	Specialized Electronic Equipment, Automotive M2M	Specialized Electronic Equipment, Automotive M2M	Industrial M2M
Certification level	–	–	–	CC EAL5+ high

Infineon: contactless communication

32-bit CPU
Cryptography
1.5MByte Flash
32KByte RAM
Myfare

	SWP UICCs			
Product name	**SLE 97CNFX8000PE** NFC Optimized SOLID FLASH™	**SLE 97CNFX1M00PE** NFC Optimized SOLID FLASH™	**SLE 97CNFX1M30PE** new NFC Optimized SOLID FLASH™	**SLE 97CNFX1M50PE** new NFC Optimized SOLID FLASH™
Product description	32-bit SWP SIM-card Security Cryptocontroller	32-bit SWP SIM-card Security Cryptocontroller	32-bit SWP SIM-card Security Cryptocontroller	32-bit SWP SIM-card Security Cryptocontroller
Interfaces	ISO 7816, SWP (Mifare compatible)	ISO 7816, SWP (Mifare compatible)	ISO 7816, SWP (Mifare compatible)	ISO 7816, SWP (Mifare compatible)
Memory	800kByte SOLID FLASH™, 32kByte RAM	1MByte SOLID FLASH™, 32kByte RAM	1.3MByte SOLID FLASH™, 32kByte RAM	1.5MByte SOLID FLASH™, 32kByte RAM
CPU	32-bit	32-bit	32-bit	32-bit
Symmetrical Cryptography	DES, 3DES, AES up to 256-bit	DES, 3DES, AES up to 256-bit	DES, 3DES, AES up to 256-bit	DES, 3DES, AES up to 256-bit
Asymmetrical Cryptography	RSA up to 4096-bit, ECC up to 521-bit	RSA up to 4096-bit, ECC up to 521-bit	RSA up to 4096-bit, ECC up to 521-bit	RSA up to 4096-bit, ECC up to 521-bit
Ambient temperature	-25 to +85°C	-25 to +85°C	-25 to +85°C	-25 to +85°C
Delivery forms	FCOS™ module, VQFN-8, Wirebond module, Chip Scale Package, Wafer sawn	FCOS™ module, VQFN-8, Wirebond module, Chip Scale Package, Wafer sawn	FCOS™ module, VQFN-8, Wirebond module, Chip Scale Package, Wafer sawn	FCOS™ module, VQFN-8, Wirebond module, Chip Scale Package, Wafer sawn
Typical applications	SWP Micro SD, SWP SIM & UICC (NFC), Mobile Payment, Embedded SIM with NFC functionality, CIPURSE™ for mobile	SWP Micro SD, SWP SIM & UICC (NFC), Mobile Payment, Embedded SIM with NFC functionality, CIPURSE™ for mobile	SWP Micro SD, SWP SIM & UICC (NFC), Mobile Payment, Embedded SIM with NFC functionality, CIPURSE™ for mobile	SWP Micro SD, SWP SIM & UICC (NFC), Mobile Payment, Embedded SIM with NFC functionality, CIPURSE™ for mobile
Certification level	CC EAL5+ high/EMVCo	CC EAL5+ high/EMVCo	CC EAL5+ high/EMVCo	CC EAL5+ high/EMVCo

Infineon: Government ID

Dual 16-bit CPU
Cryptography
600kByte Flash
12KByte RAM
Dual interface

	Dual-interface & Contactless Security Controller [1]			
Product name	**SLE 78CLFX5000PH** Integrity Guard, Mega Memory, SOLID FLASH™	**SLE 78CLFX500VPH** Integrity Guard, VHBR, SOLID FLASH™, Mega Memory	**SLE 78CLFX6280PH** new Integrity Guard, Mega Memory, SOLID FLASH™	**SLE 78CLFX628VPH** new Integrity Guard, VHBR, SOLID FLASH™, Mega Memory
Product description	Dual-interface and Contactless Security Cryptocontroller	Dual-interface and Contactless Security Cryptocontroller	Dual-interface and Contactless Security Cryptocontroller	Dual-interface and Contactless Security Cryptocontroller
Interfaces	ISO 7816, ISO 14443 A/B, ISO 18092 passive mode, Mifare compatible interface	ISO 7816, ISO 14443 A/B, ISO 18092 passive mode, Mifare compatible interface, Very High Bit Rates (VHBR) with up to 6.8Mbit/s	ISO 7816, ISO 14443 A/B, ISO 18092 passive mode, Mifare compatible interface	ISO 7816, ISO 14443 A/B, ISO 18092 passive mode, Mifare compatible interface, Very High Bit Rates (VHBR) with up to 6.8Mbit/s
Memory	500kByte SOLID FLASH™, 12kByte RAM	500kByte SOLID FLASH™, 12kByte RAM	628kByte SOLID FLASH™, 12kByte RAM	628kByte SOLID FLASH™, 12kByte RAM
CPU	Dual 16-bit	Dual 16-bit	Dual 16-bit	Dual 16-bit
Crypto coprocessor symmetrical	DES, 3DES, AES up to 256-bit	DES, 3DES, AES up to 256-bit	DES, 3DES, AES up to 256-bit	DES, 3DES, AES up to 256-bit
Crypto coprocessor asymmetrical	RSA up to 4096-bit, ECC up to 521-bit	RSA up to 4096-bit, ECC up to 521-bit	RSA up to 4096-bit, ECC up to 521-bit	RSA up to 4096-bit, ECC up to 521-bit
Ambient temperature	-25 to +85°C	-25 to +85°C	-25 to +85°C	-25 to +85°C
Delivery forms	Dual interface module, Contactless module, Wafer sawn	Dual interface module, Contactless module, Wafer sawn	Dual interface module, Contactless module, Wafer sawn	Dual interface module, Contactless module, Wafer sawn
Typical applications	National eID, ePassport, eHealth card/eSocial card, eDriver's License, eVisa, eResidence Permit, eTachograph, eVehicle Registration Card/eCar Registration, eSignature	National eID, ePassport, eHealth card/eSocial card, eDriver's License, eVisa, eResidence Permit, eTachograph, eVehicle Registration Card/eCar Registration, eSignature	National eID, ePassport, eHealth card/eSocial card, eDriver's License, eVisa, eResidence Permit, eTachograph, eVehicle Registration Card/eCar Registration, eSignature	National eID, ePassport, eHealth card/eSocial card, eDriver's License, eVisa, eResidence Permit, eTachograph, eVehicle Registration Card/eCar Registration, eSignature
Certification level	CC EAL6+ high/EMVCo	CC EAL6+ high/EMVCo	CC EAL6+ high/EMVCo	CC EAL6+ high/EMVCo

Infineon: USB tokens

32-bit CPU
Cryptography
500kByte Flash
24KByte RAM
USB interface

	USB Tokens (32-bit)		
SLE 78CLUX5007PH [1)] Integrity Guard SOLID FLASH™	**SLE 97CUFX5000PH** SOLID FLASH™	**SLE 97CUFX500FPH** SOLID FLASH™	**SLE 97CUSIFX5000PH** SOLID FLASH™
Multi-Interface USB-Security Cryptocontroller with a contactless interface	USB-Security Cryptocontroller	USB-Security Cryptocontroller for use in a chipcard formfactor	Multi-Interface USB-Security Cryptocontroller
USB 2.0, GPIO, I2C, SPI, ISO 7816, ISO 14443 A/B, ISO 18092 passive mode, Mifare compatible interface, Sub-ID1 optimized product	USB 2.0, ISO 7816	USB 2.0, ISO 7816	USB 2.0, GPIO, I2C, SPI, ISO 7816
500kByte SOLID FLASH™, 182kByte ROM, 16kByte RAM	504kByte SOLID FLASH™, 20kByte RAM	504kByte SOLID FLASH™, 20kByte RAM	504kByte SOLID FLASH™, 24kByte RAM
Dual 16-bit	32-bit	32-bit	32-bit
DES, 3DES, AES up to 256-bit	DES, 3DES, AES up to 256-bit	DES, 3DES, AES up to 256-bit	DES, 3DES, AES up to 256-bit
RSA up to 4096-bit, ECC up to 521-bit	RSA up to 4096-bit, ECC up to 521-bit	RSA up to 4096-bit, ECC up to 521-bit	RSA up to 4096-bit, ECC up to 521-bit
-25 to +85°C	-25 to +85°C	-25 to +85°C	-25 to +85°C
VQFN32-13, Wafer sawn	VQFN32-13, Wafer sawn	Contact-based module, Wafer sawn	VQFN32-13, Wafer sawn
USB Tokens	USB Tokens	USB Tokens	USB Tokens
CC EAL6+ high/EMVCo	CC EAL5+ high/EMVCo	CC EAL5+ high/EMVCo	CC EAL5+ high/EMVCo

Infineon: Ticketing (NFC)

small CPU
No Cryptography
1KByte Flash
NFC interface

	Mifare compatible, my-d™ proximity and ticketing products			
Product name	**SLE 66R16S my-d™ proximity**	**SLE 66R32S my-d™ proximity**	**SLE 66R04S my-d™ proximity**	**SLE 66R35(I)(R)(E7) Fully Mifare Compatible**
Product description	Security memory with authentication, 2560Byte EEPROM	Security memory with authentication, 5120Byte EEPROM	Security memory with authentication, 770Byte EEPROM	Intelligent 1kByte EEPROM using Mifare technologies, (I) = Supporting 4-byte fixed number, non unique ID (R) = Supporting 4-byte reused ID, (E7) = Supporting 7-byte UID
Interface	ISO/IEC 14443-3 Type A	ISO/IEC 14443-3 Type A	ISO/IEC 14443-3 Type A	ISO/IEC 14443-3 Type A
Memory organization	Up to 15 sectors fully configurable (14 secure, 1 plain)	Up to 15 sectors fully configurable (14 secure, 1 plain)	Up to 15 sectors fully configurable (14 secure, 1 plain)	16 fixed sectors
Counter	Up to 65,536 units, support of anti-tearing	Up to 65,536 units, support of anti-tearing	Up to 65,536 units, support of anti-tearing	–
EEPROM - user	2008Byte	4056Byte	576Byte	768Byte
EEPROM - administration	552Byte	1064Byte	194Byte	256Byte
Security features	Transport key, Unique serial number, Mutual authentication with 64-bit keys, Hierarchical key management	Transport key, Unique serial number, Mutual authentication with 64-bit keys, Hierarchical key management	Transport key, Unique serial number, Mutual authentication with 64-bit keys, Hierarchical key management	Transport key, Mutual three pass authentication with 48-bit keys
Distance (read/write)	Typically up to 10cm and above	Typically up to 10cm and above	Typically up to 10cm and above	Typically up to 10cm and above
Data rate	106kbit/s to card up to 848kbit/s to reader	106kbit/s to card up to 848kbit/s to reader	106kbit/s to card up to 848kbit/s to reader	106kbit/s
Endurance	100,000	100,000	100,000	100,000
Retention time, minimum	10 years	10 years	10 years	10 years
Delivery forms	Wafer sawn, NiAu-bump, MCC2, MCC8	Wafer sawn, NiAu-bump, MCC2, MCC8	Wafer sawn, NiAu-bump, MCC2, MCC8	Wafer sawn, NiAu-bump, MCC2, MCC8
Tools	Evaluation Kit Contactless	Evaluation Kit Contactless	Evaluation Kit Contactless	Evaluation Kit Contactless
Typical applications	Public Transport, Ticketing	Public Transport, Ticketing	Public Transport, Ticketing	Public Transport, Ticketing, Access Management

Infineon: Internet of Things (IoT)

small CPU
No Cryptography
10kByte Flash
Wireless interface

	my-d™ vicinity plain			
Product name	**SRF 55V02P**	**SRF 55V02P HC**	**SRF 55V10P**	**SRF 55V10P HC**
Product description	Plain memory, 2.5kbit EEPROM	Plain memory, 2.5kbit EEPROM	Plain memory, 10kbit EEPROM	Plain memory, 10kbit EEPROM
Interface	ISO/ IEC 18000-3 mode 1	ISO/ IEC 18000-3 mode 1	ISO/ IEC 18000-3 mode 1	ISO/ IEC 18000-3 mode 1
Memory organization	1 fixed sector	1 fixed sector	1 fixed sector	1 fixed sector
Counter	Up to 65,536 units, support of anti-tearing	Up to 65,536 units, support of anti-tearing	Up to 65,536 units, support of anti-tearing	Up to 65,536 units, support of anti-tearing
EEPROM - user	224Byte	224Byte	992Byte	992Byte
EEPROM - administration	64Byte	64Byte	256Byte	256Byte
Security features	Unique serial number, Individual page locking	Unique serial number, Individual page locking	Unique serial number, Individual page locking	Unique serial number, Individual page locking
Distance (read/write)	Typically up to 1.5m	Typically up to 1.5m	Typically up to 1.5m	Typically up to 1.5m
Data rate	26.48kbit/s	26.48kbit/s	26.48kbit/s	26.48kbit/s
Endurance	100,000	100,000	100,000	100,000
Retention time, minimum	10 years	10 years	10 years	10 years
Delivery forms	Wafer sawn, NiAu-bump, MCC2, MCC8	Wafer sawn, NiAu-bump, MCC2, MCC8	Wafer sawn, NiAu-bump, MCC2, MCC8	Wafer sawn, NiAu-bump, MCC2, MCC8
Tools	Evaluation Kit Contactless	Evaluation Kit Contactless	Evaluation Kit Contactless	Evaluation Kit Contactless
Typical applications	Inventory Control, Libraries	CD Inlays, Laundry	Inventory Control, Libraries	Factory Automation, Inventory Control

ISO 7816 Standards

7816/1: Physical characteristics

- Specifies the physical and dimensional features of the plastic supports. Additional characteristics specified are Mechanical strength, Static electricity, Electromagnetic fields and Bending properties etc.

7816/2: Dimensions and location of the contacts

- This part defines eight contact referred to as C1 to C8. The contacts are located as shown in figure below.

7816/3: Electronic signals and transmission protocols

- Specifies electronics signals and transmission protocols that the DC electrical characteristics, the character format and the command protocol for the Smart Card.
- This ISO standard describes two types of data transfer between Smart Card and card Reader/Writer:
  - asynchronous protocol with two data coding conventions
  - synchronous protocol

7816/4: Industry commands for interchange

- The content of the message, commands and responses, transmitted by the interface device to the card and conversely.
- The structure and content of the historical bytes sent by the card during the answer to reset.
- The structure of files and data, as seen at the interface when processing inter-industry commands for interchange.
- Access methods to files and data in the card.
- A security architecture defining access rights to files and data in the card.
- Methods for secure messaging

7816/5: Number system and registration procedure for application identifiers

7816/6: Inter-industry data elements

Information Technology Security Evaluation Criteria
(ITSEC) - Europe

EAL1 – functional tested

EAL2 – structurally tested

EAL3 – methodologically tested and checked

EAL4 - methodologically designed, and tested

EAL5 – semi-formally designed and tested

EAL6 – semi-formally verified designed and tested

EAL7 -formally verified designed and tested

NORTHERN ARIZONA UNIVERSITY

4 Smartcards and Secure elements

- 1 General description
  - Why smartcards?
  - Microprocessor cards with crypto-processor
  - Contactless and combi cards
- 2 Security services
  - Cryptographic services, principles, and algorithms
- 3 Software
  - Operating systems
  - Javacard

Security with smart cards

Any ***secure transaction*** with smart cards involves the following generic functions:

- ❑*Data Protection*
- ❑*Identification of the cardholder / Mutual authentication*
- ❑*Secure writing*
- ❑*Certification or digital signature*
- ❑*Encryption*

The transmission between card and outside world is ***protected by cryptography*** for***:***

- ❑*Writing operation*
- ❑*Authentication the card or the terminal*
- ❑*Origin of the message*
- ❑*Transmission of cryptographic keys*

Smart cards ***prevent unauthorized*** users from gaining access to ***stored information***.

The chip can ***store and process passwords and PINs***.

The ***password is not sent over a communication line*** for verification.

The important part of a smart card is the ***software that provide the applications***.

Authentication with smartcards

PIN (Personal Identification Number)

- PINs can be stolen or abused
- Entropy of 13-20 [4 digits=10^4 config. ➔ $Ln_2(10^4) \approx 13.3$]
  [6 digits=10^6 config. ➔ $Ln_2(10^6) \approx 20$]

Multi-factor authentication:

- **Biometrics**:
  - Fingerprint and vein-print
  - Iris and Retinal scans,
  - Facial recognition
- **Hardware authentication**
  - Physically unclonable Functions

Other authentication methods

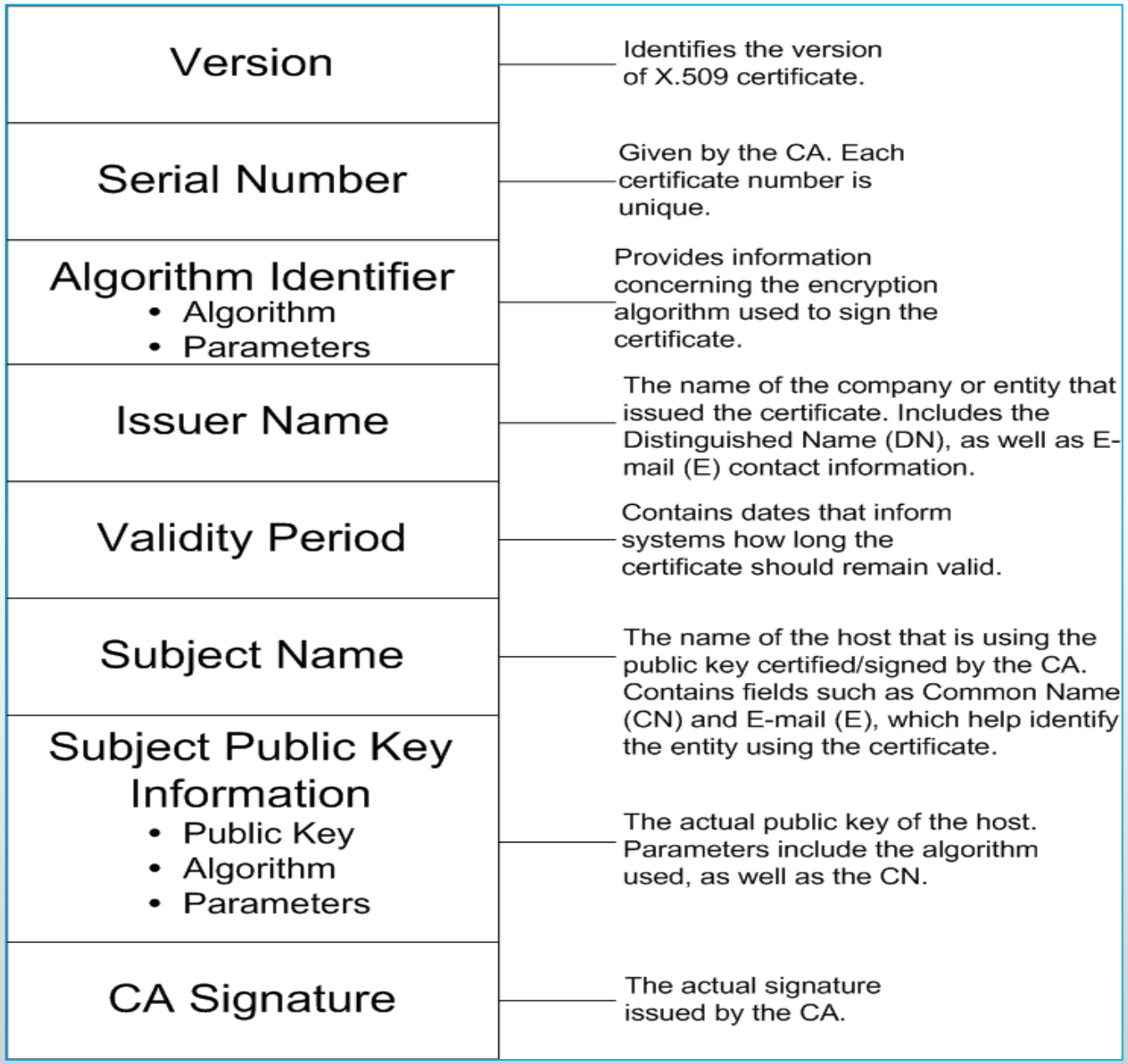
- User behavior, and profile [Big data analysis - Machine learning]
- Cryptography: PKI [private keys] , one time password,…

Electronic Signatures with smart cards

- **Why smartcard?:** eliminate problems related to the private key distribution, and their protection.
- **Electronic signatures** are combined with **public key infrastructure**.
- Loaded with private key(s), public key certificates and some ways to point securely to **non-repudiation** policies
- APIs allow electronic signature **enabled applications** to interface with any kind of smart card
- **Blind signatures** allow privacy features to be built into applications.

E-cash uses blind signatures & offer payer anonymity.

Public Key Infrastructure (PKI) – X.509



Smart Card Life Cycle

Phases	Fabrication	Pre-personalisation	Personalisation	Utilization	End of Life
Access mode	***Physical*** *addressing*		***Logical*** *addressing*		
System	*Part of the chip design*		*Not accessible*		
Key generation	*Write card ID*	*Write Private Keys*	*Not accessible*		
Fabrication data	*Read/write/erase*	*Read*	*Read*		
Directory	*Read/write/erase*		*According to logical file access conditions*		
Data	*Read/write/erase*		*According to logical file access conditions*		
Optional code	*Read/write/erase*		*Not accessible*		

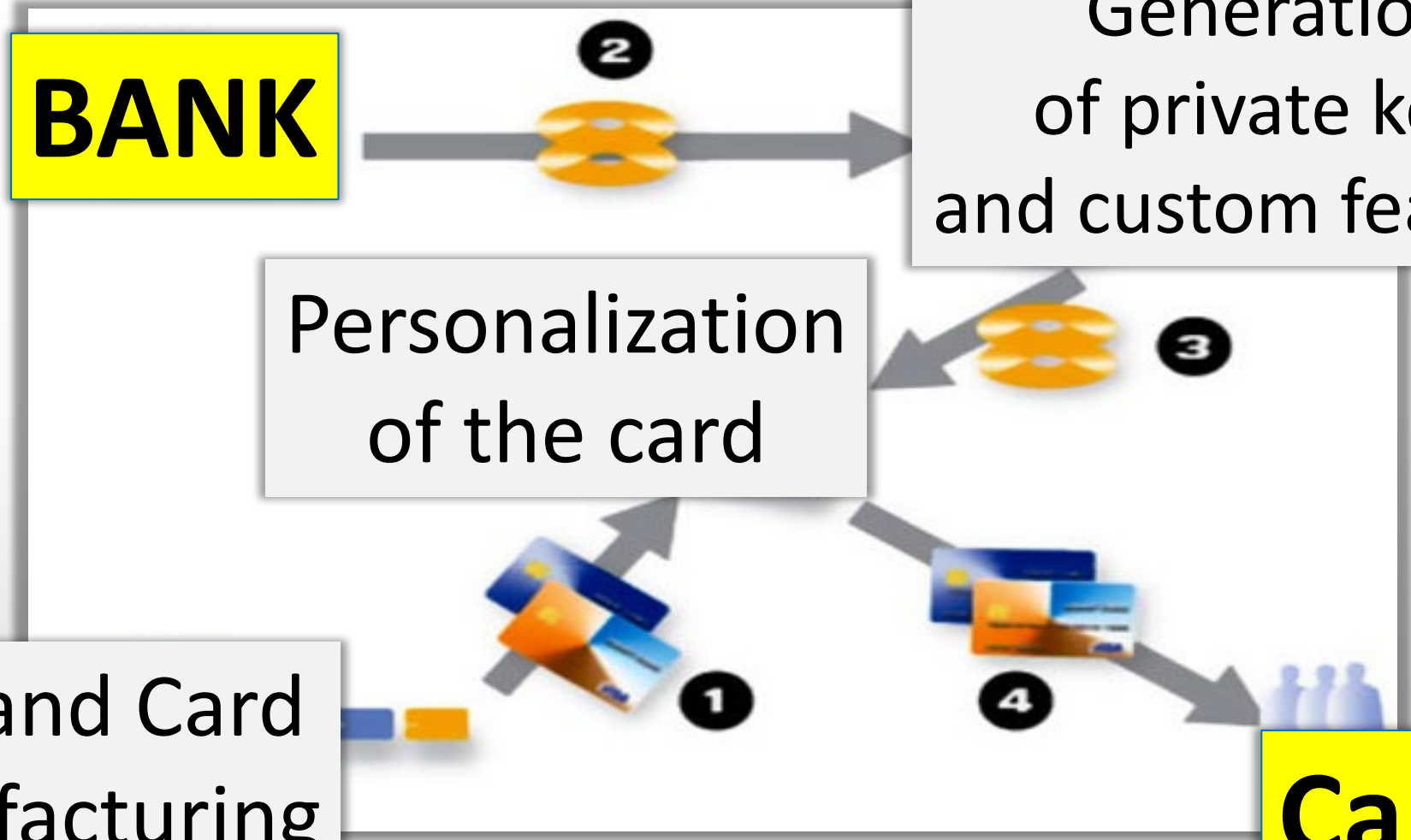
Secure manufacturing ***Non secure environment***

Card Production tracking

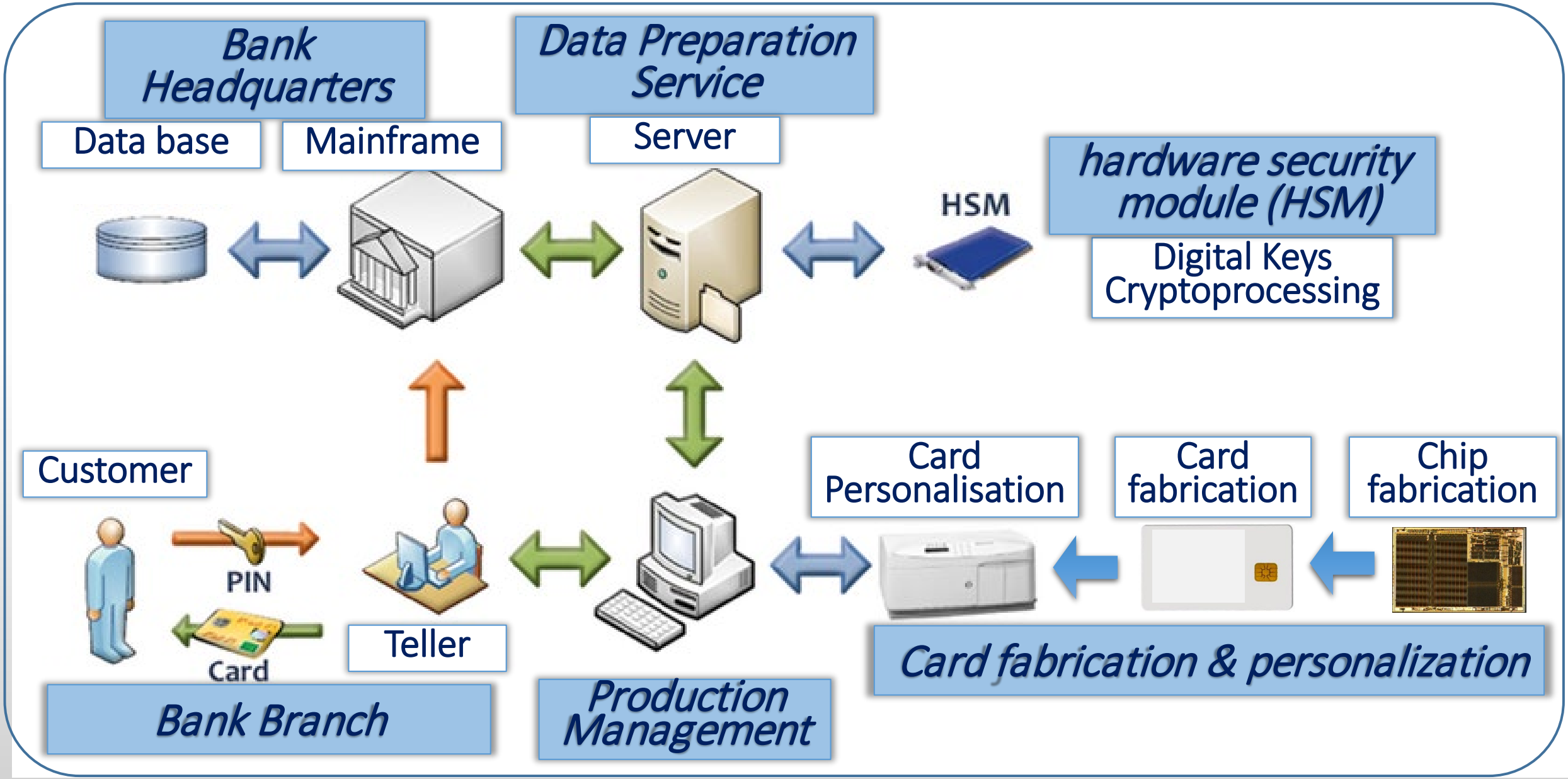
CPLC info

IC Fabricator: **4790**
IC Type: **5167**
OS ID: **4791**
OS Release Date: **2081**
OS Release Level: **3b00**
IC Fabrication Date ((Y DDD) date in that year): **4126**
IC Serial Number: **00865497**
IC Batch Identifier: **3173**
IC Module Fabricator: **4812**
IC Module Packaging Date: **4133**
IC Manufacturer: **0000**
IC Embedding Date: **0000**
IC Pre Personalizer: **1017**
IC Pre Personalization Equipment Date: **4230**
IC Pre Personalization Equipment ID: **38363534**
IC Personalizer: **0000**
IC Personalization Date: **0000**
IC Personalization Equipment ID: **00000000**

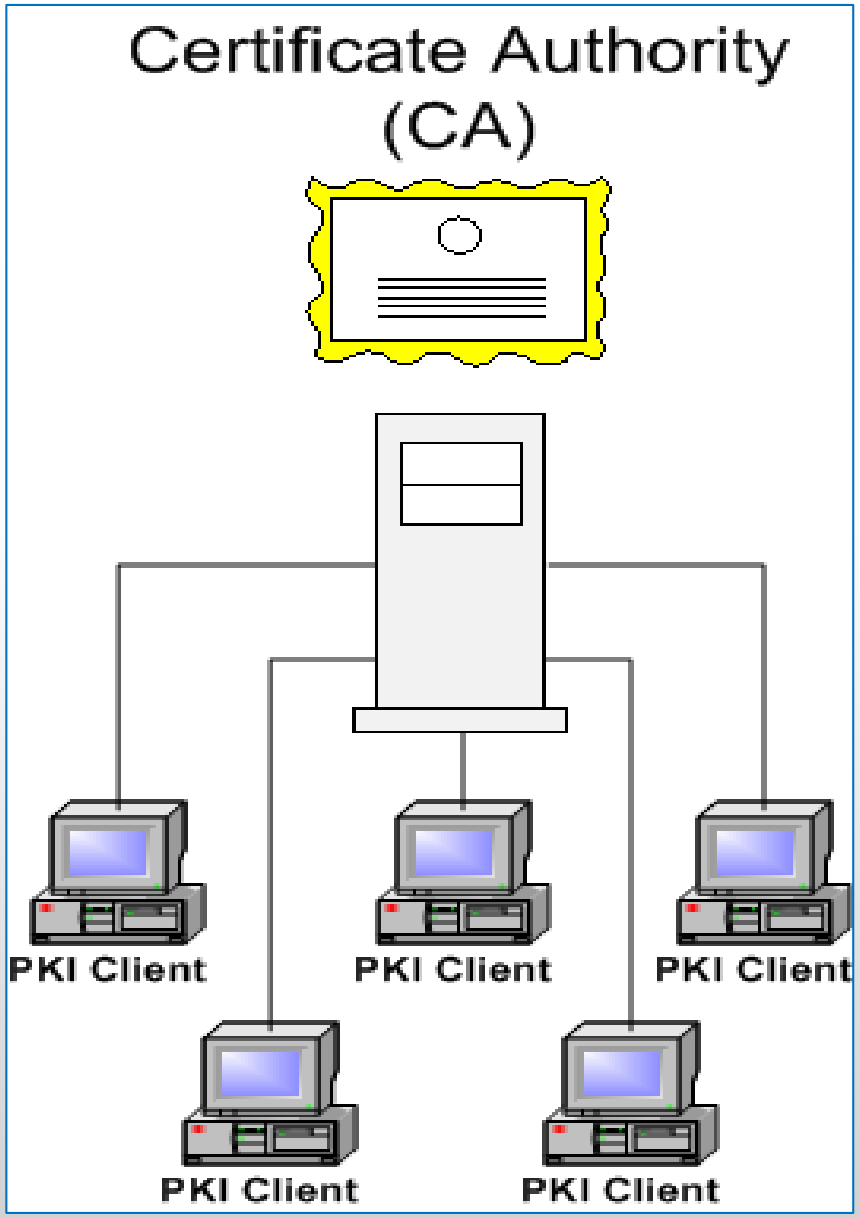
Banking card personalization process

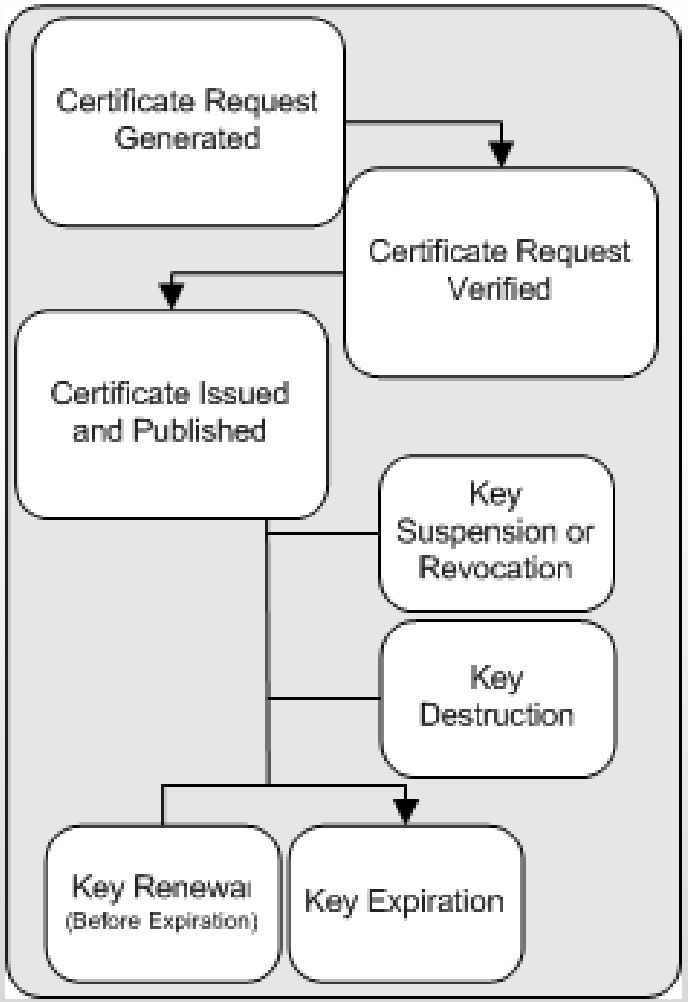


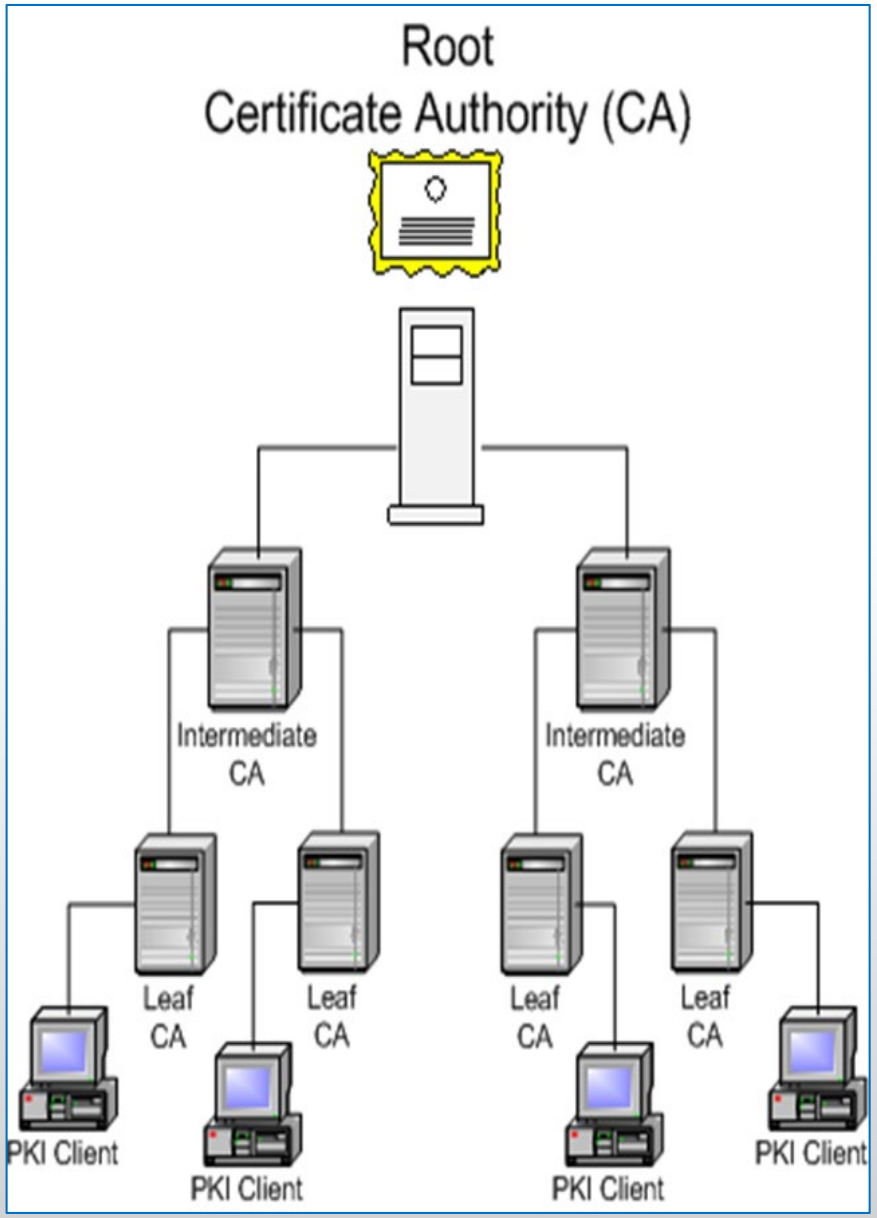
Detailed card personalization process



Key Management and the Certificate Life Cycle



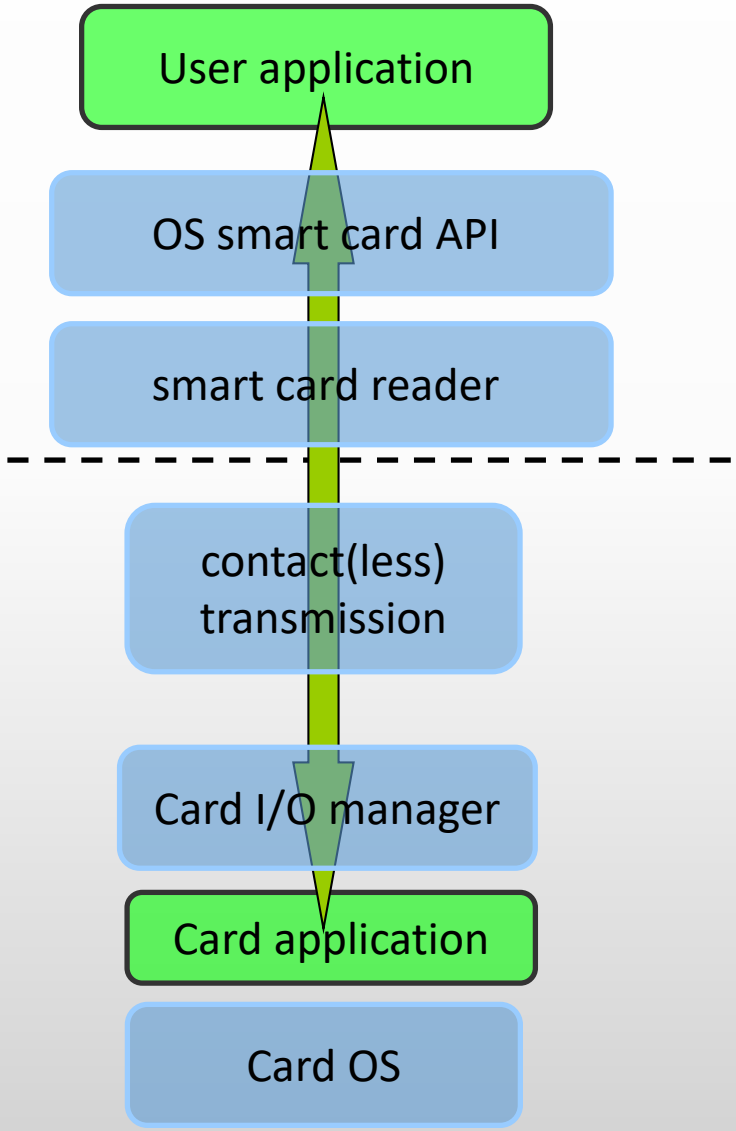




4 Smartcards and Secure elements

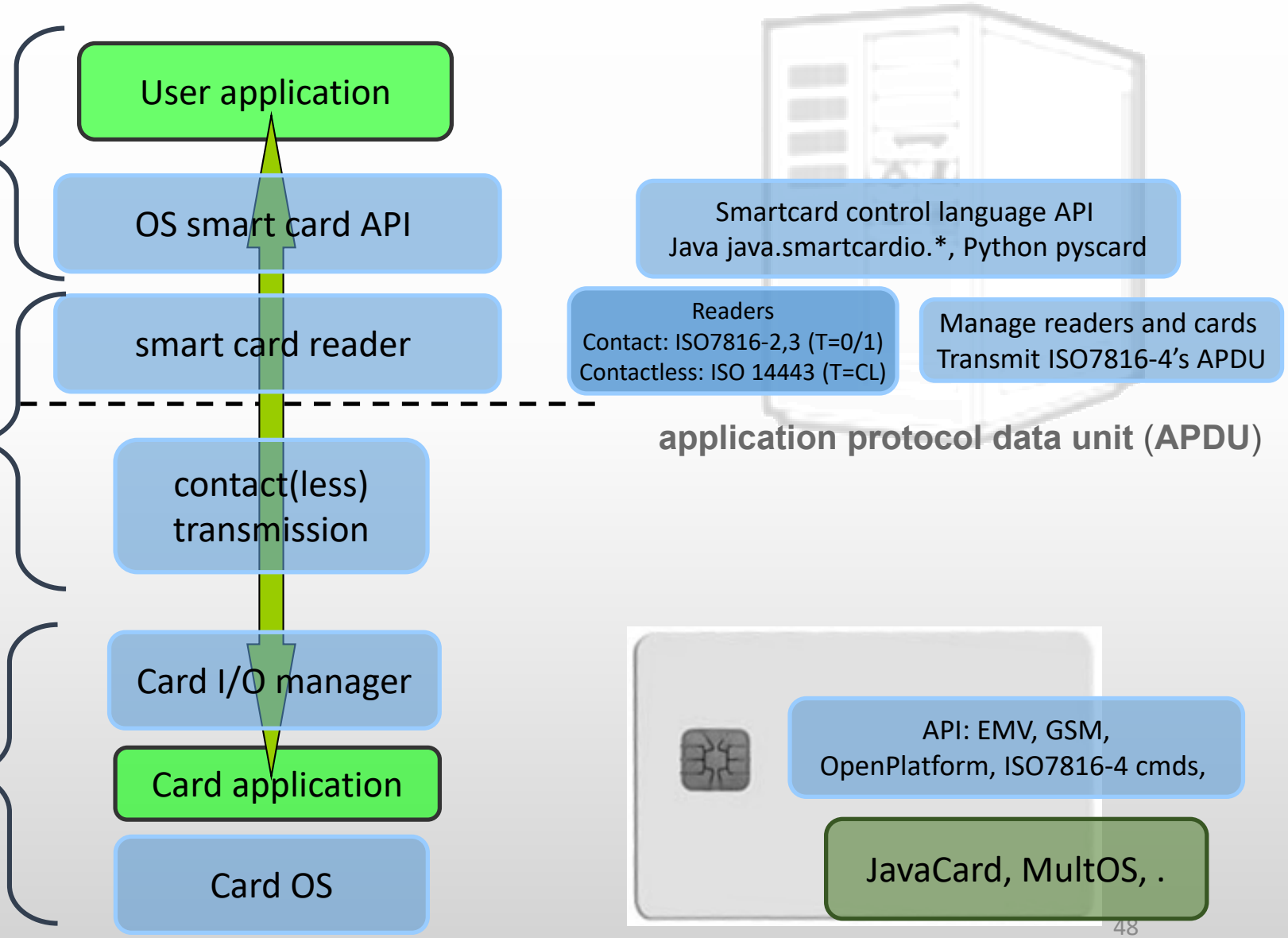
- 1 General description
  - Why smartcards?
  - Microprocessor cards with crypto-processor
  - Contactless and combi cards
- 2 Security services
  - Cryptographic services, principles, and algorithms
- 3 Software
  - Operating systems
  - Javacard

Smart card Software components

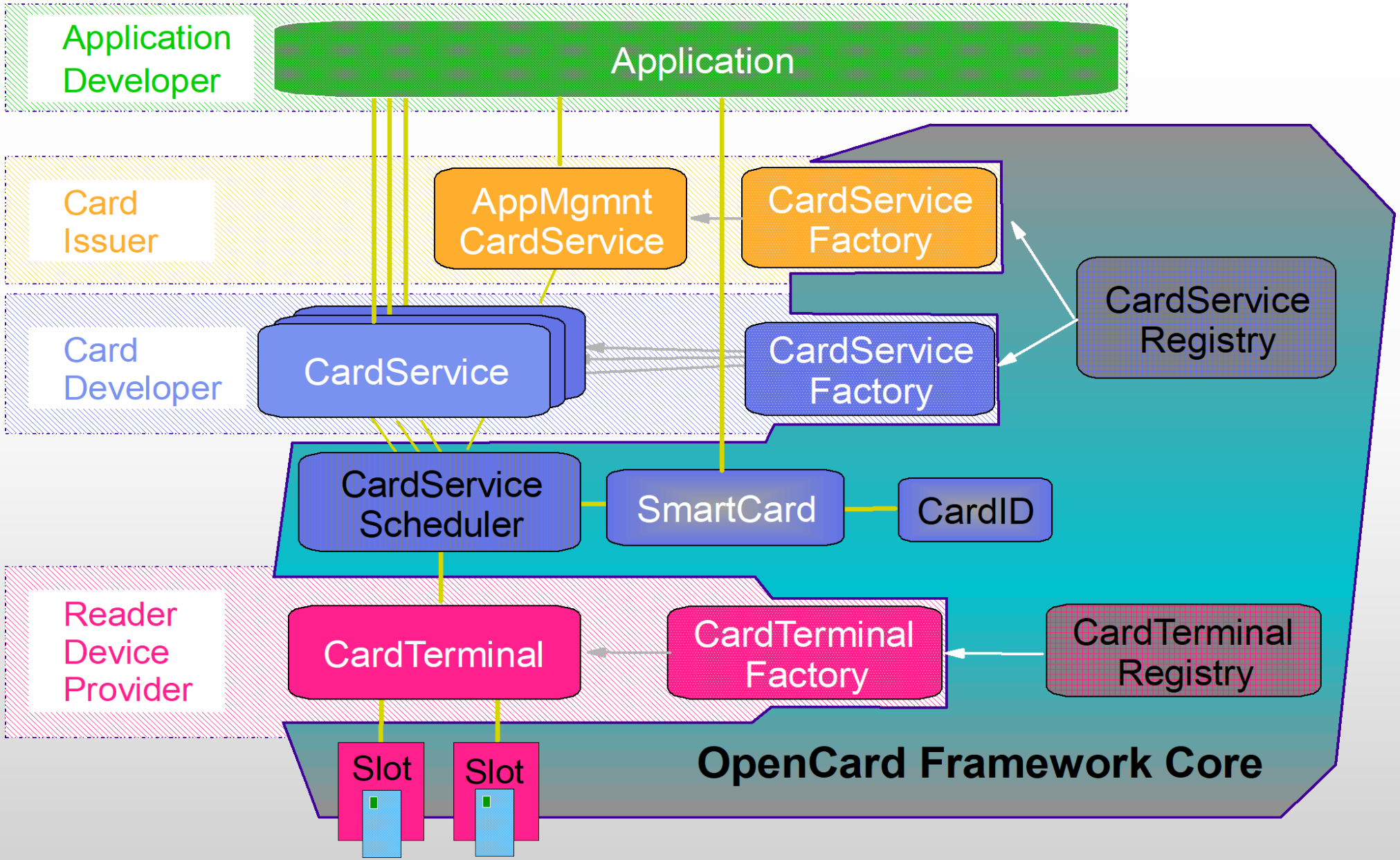


Card programming platforms

- *GlobalPlatform (Ex: open card forum (OCF)*
  - remote card management interface
  - secure installation of applications
- *PKCS#11*
  - standardized interface on host side
  - card can be proprietary
- *PC/SC, PC/SCLite (host side)*
  - Readers/cards management
  - Transmission of logical APDU packets
  - C/C# WinSCard.h, Java java.smartcardio.*, Python pyscard
- *ISO7816 1-4*
  - Card physical properties ISO7816-1
  - Physical layer communication protocol ISO7816-2-3
  - Data packet format (APDU)

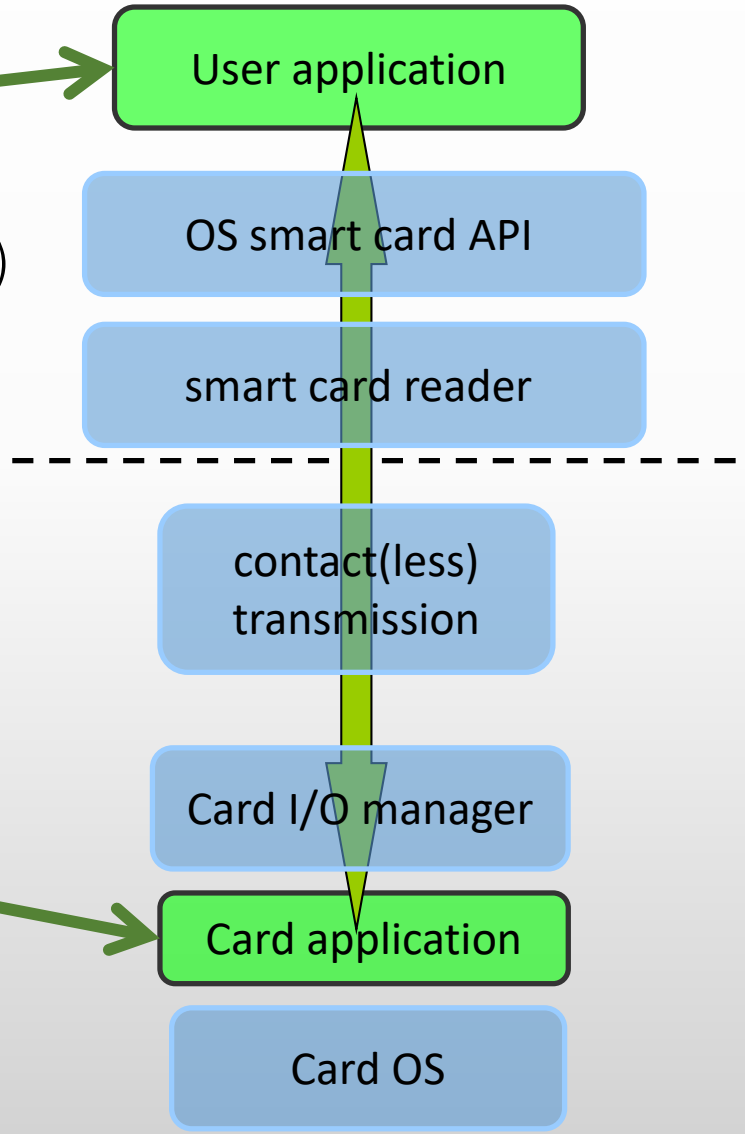


Developments - Open Card Framework (OCF)



Software – applicative environment

- *User application*
  - Card management system
  (also called client management system)
  - Merchant terminal GUI
  - Banking transfer GUI
  - Browser TLS
  - …
- *Card application*
  - EMV applet for payments
  - SIM applet for GSM
  - OpenPGP applet for PGP
  - …



OS Based Classification

Smart cards are classified on the basis of their Operating System:

- MultOS
- JavaCard
- MFC (MyFare)
- Others: Cyberflex, StarCOS,…….

Smart Card Operating Systems or SCOS, are placed on the ROM

- 10-50 KB.

SCOS handle:

- File Handling and Manipulation
- Memory Management
- Data Transmission Protocols.
- Generic Application Product Interface (API)

Common security algorithms for the crypto-processor

Truly random number generator TRNG

- RNG, PRNG, TRNG

Symmetric encryption

- 3DES,
- AES128/256

Hash function

- SHA1, SHA-2 256/512

Public key encryption

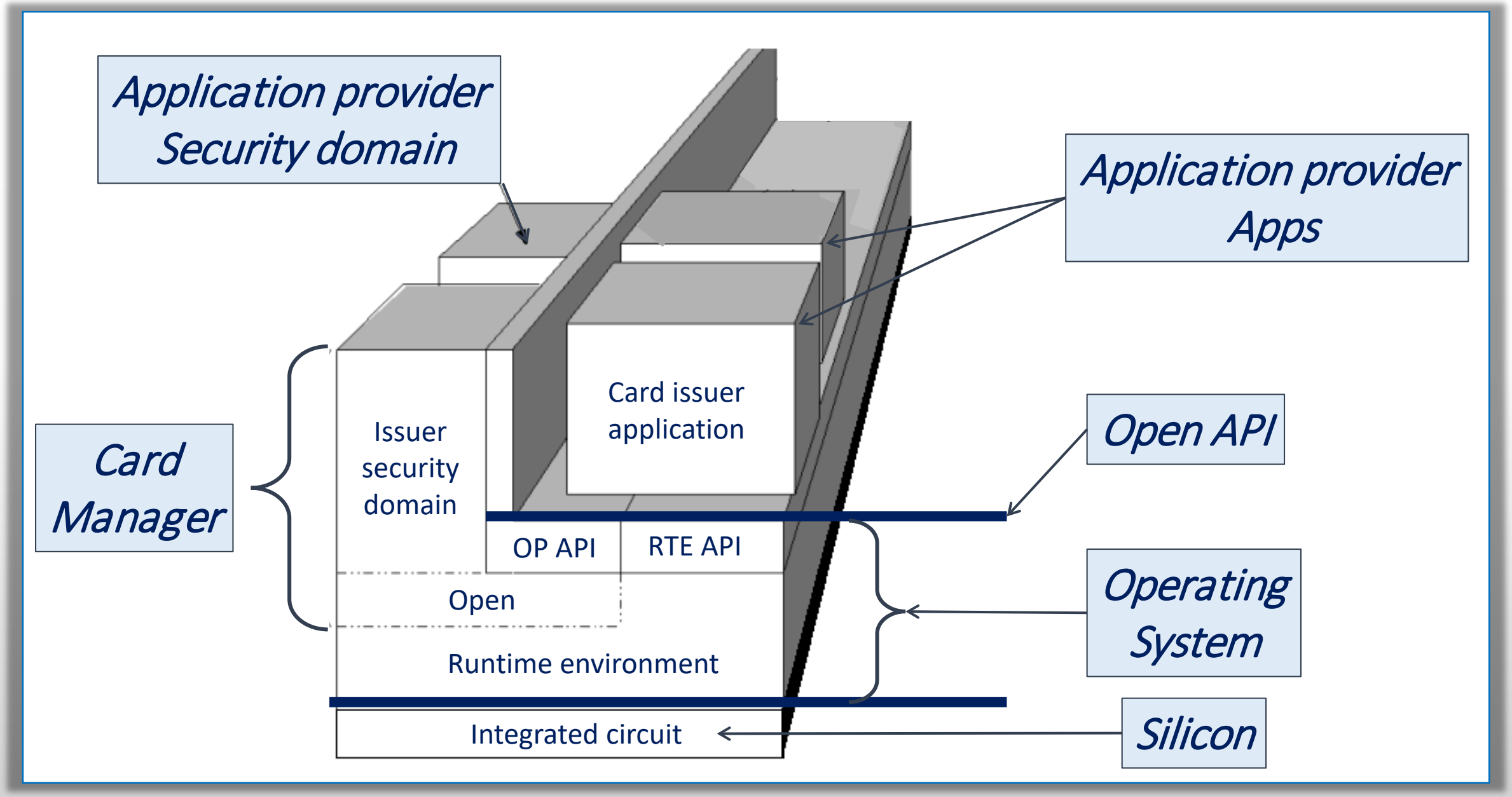
- RSA (up to 2048b common, 4096 possible)
- ECC (up to 192b common, 384b possible)
- Diffie-Hellman key exchange (DH/ECDSA) for ECC

OS protection

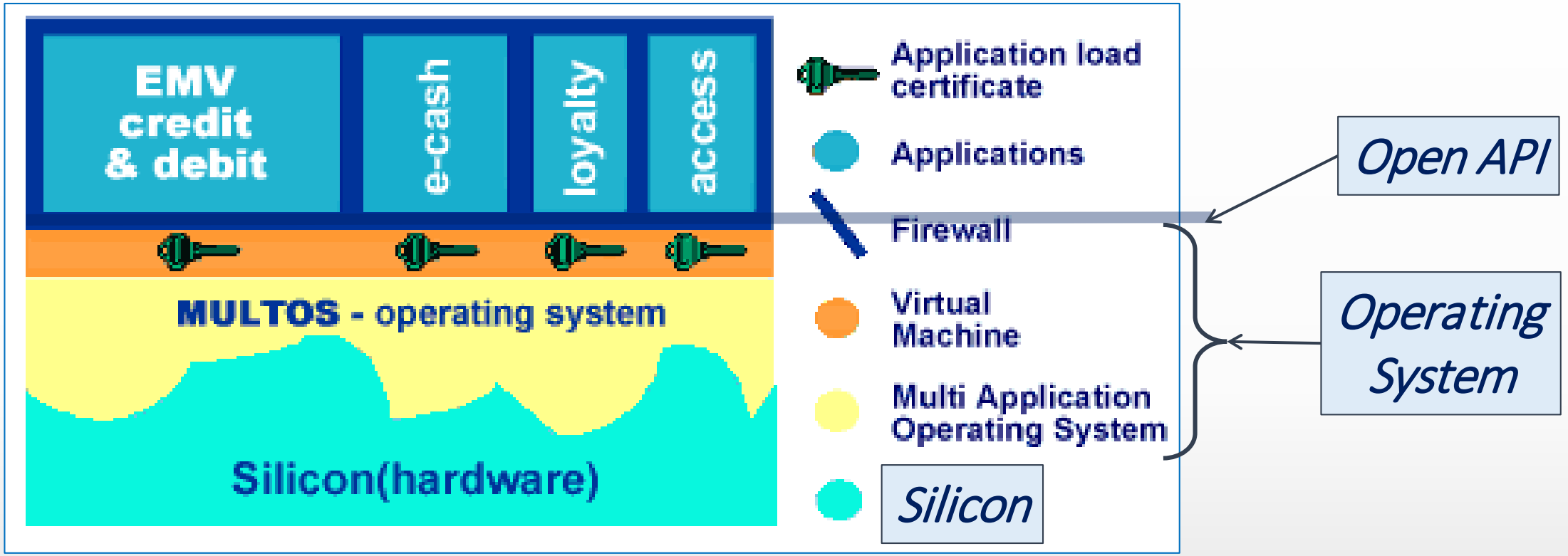
Typical speed of operation is:

- Milliseconds (RNG, symmetric crypto, hash)
- Tens of milliseconds (transfer data in/out)
- Hundreds of millisecond (asymmetric crypto)
- Seconds (RSA keypair generation)

Open Platform Card Specification

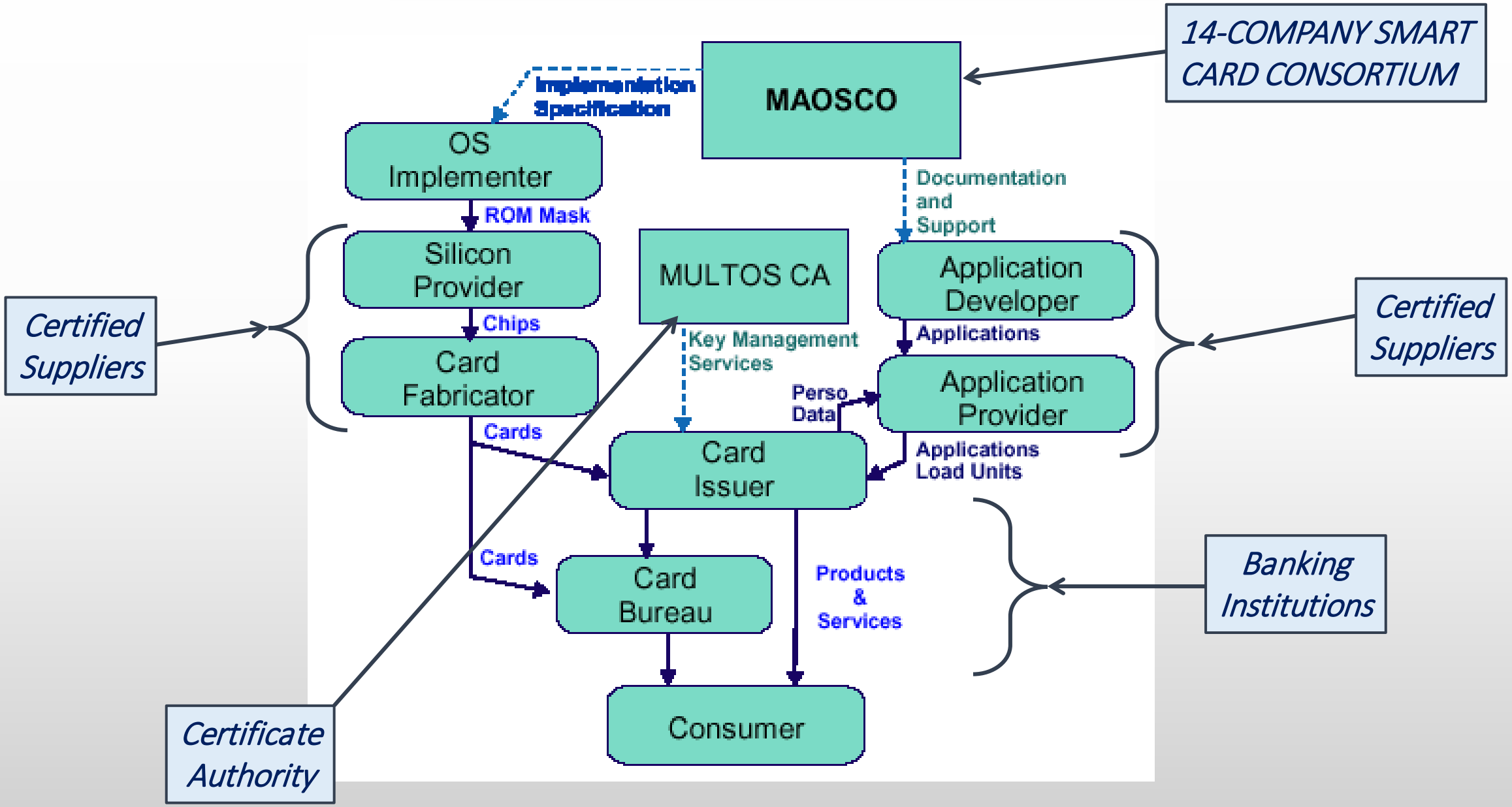


MULTOS



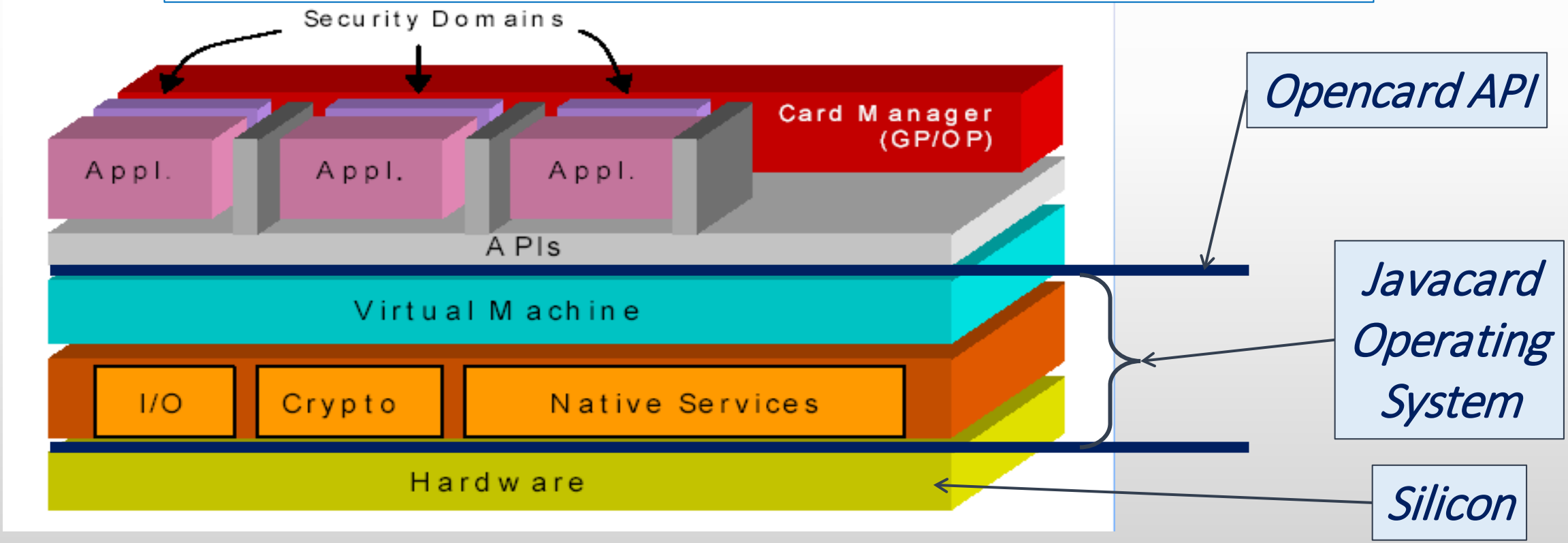
- A *high security* architecture
- Multiple, inter-operable, *platform independent applications*
- Remote loading and deletion of applications over the lifetime of a card
  Achieved using the language MEL (MULTOS Executable Language)

MULTOS Administration

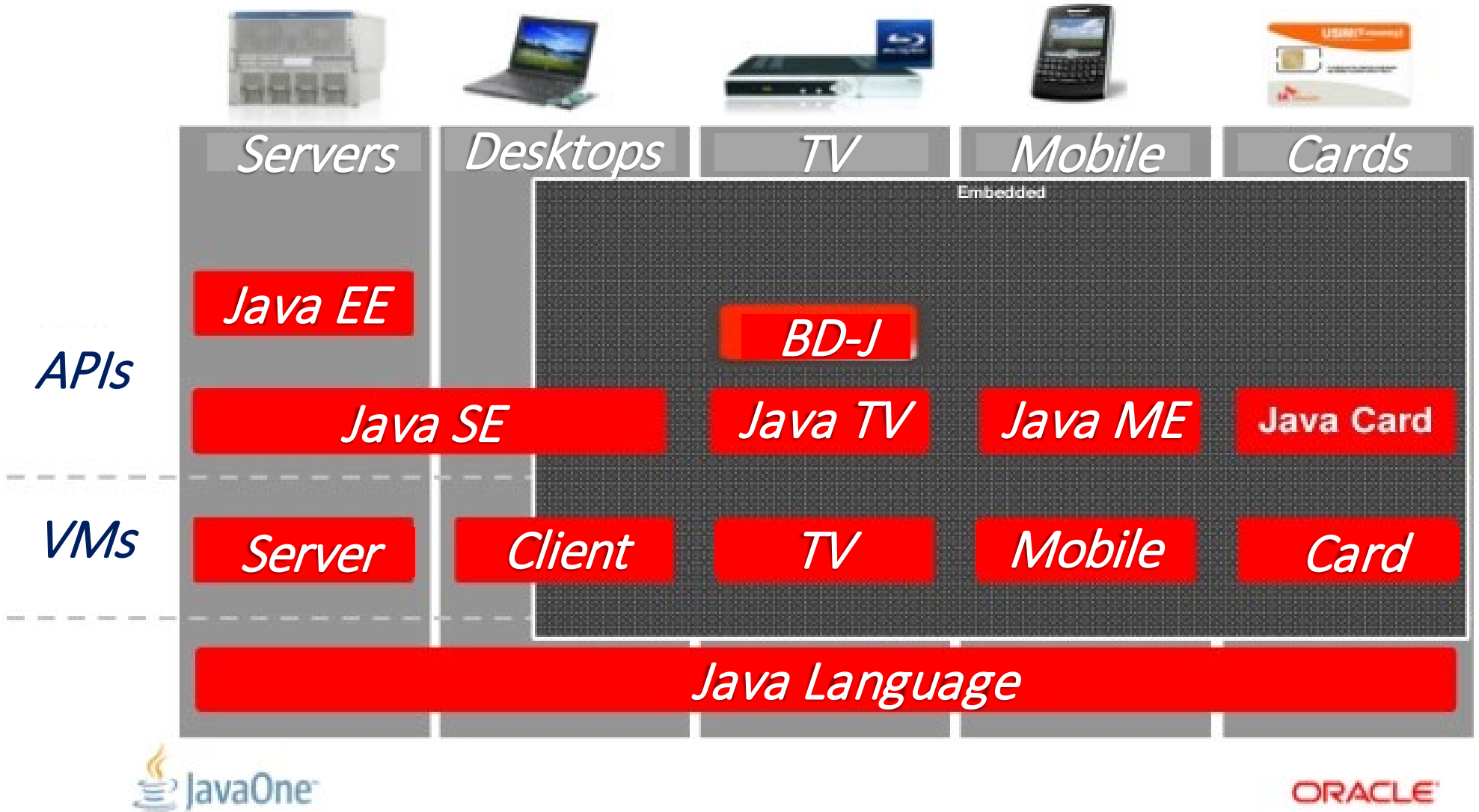


OpenCard Framework

- *Based on Java Card Architecture*
- *OpenCard is an API* that defines several of these interfaces
- Can start a Java card agent whenever the card is inserted
- To use card, must be able to open and read
- Can then communicate with applications on card during session



Oracle Java Platforms



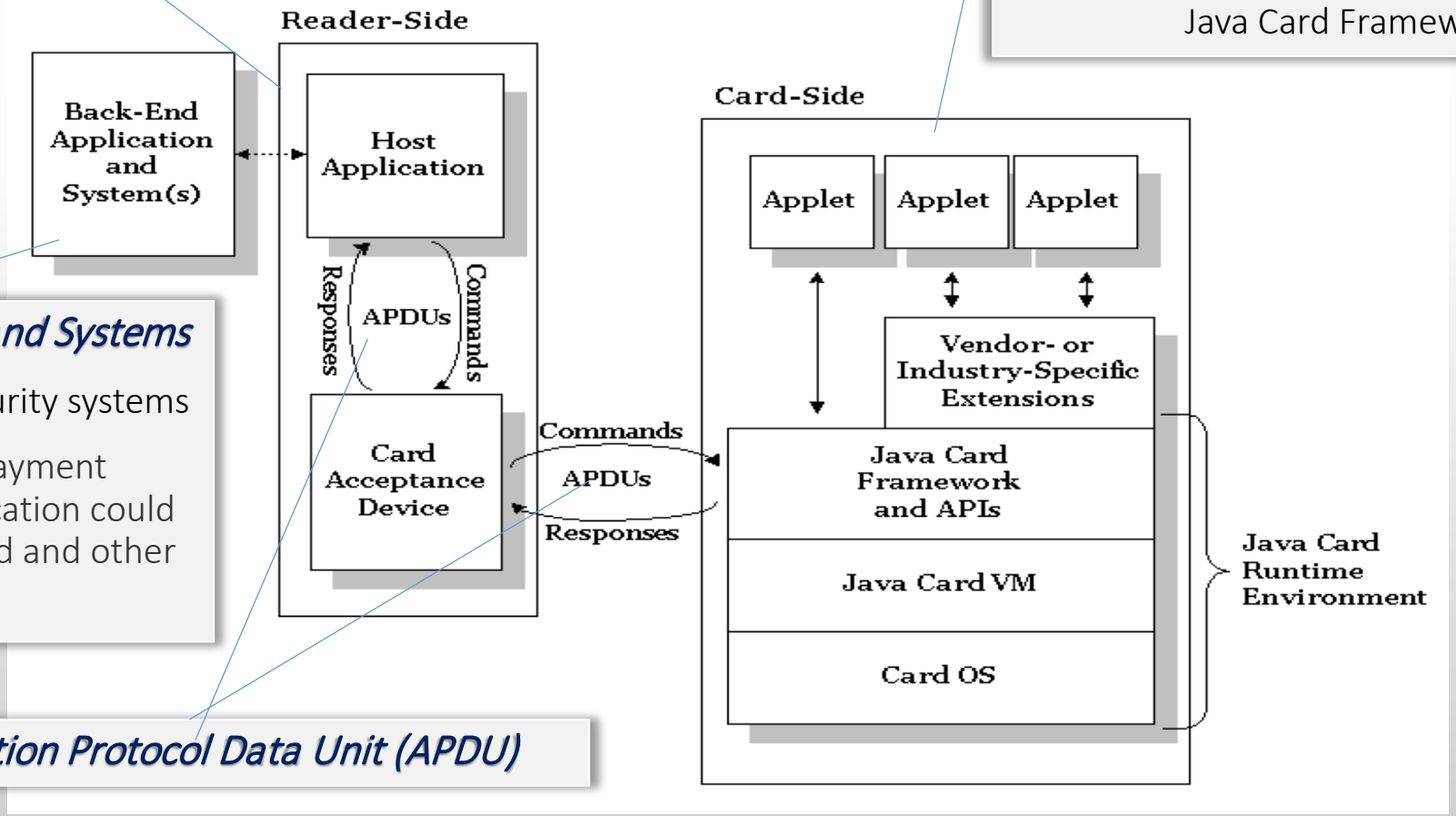
Block diagram – Java Software integration

The Reader-Side

- Consists of two parts: Host Application; Card Acceptance Device
- Think of a bank machine: *Host Application* as the Computer that provides interaction with the system. *Card Acceptance* Device being where you put your debit card in

The Card Side

- One or more Java Applets
- Card's operating System
- Java Card Runtime Environment(JCRE)
  - Java Card Virtual Machine
  - Java Card Framework and APIs

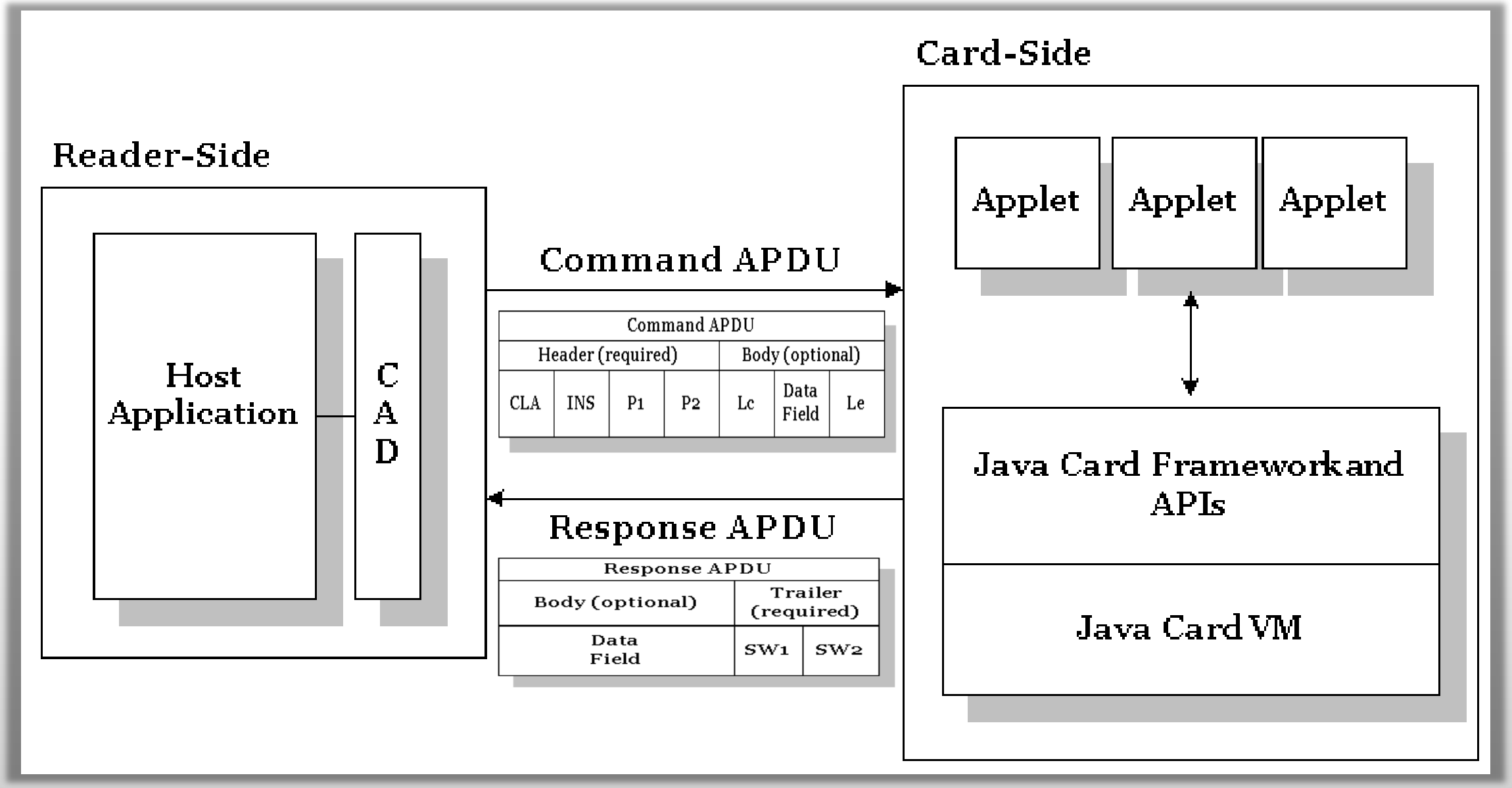


The Back-End Application and Systems

- Provide connectivity to security systems
- Example: In an electronic payment system, the back-end application could provide access to credit card and other payment information

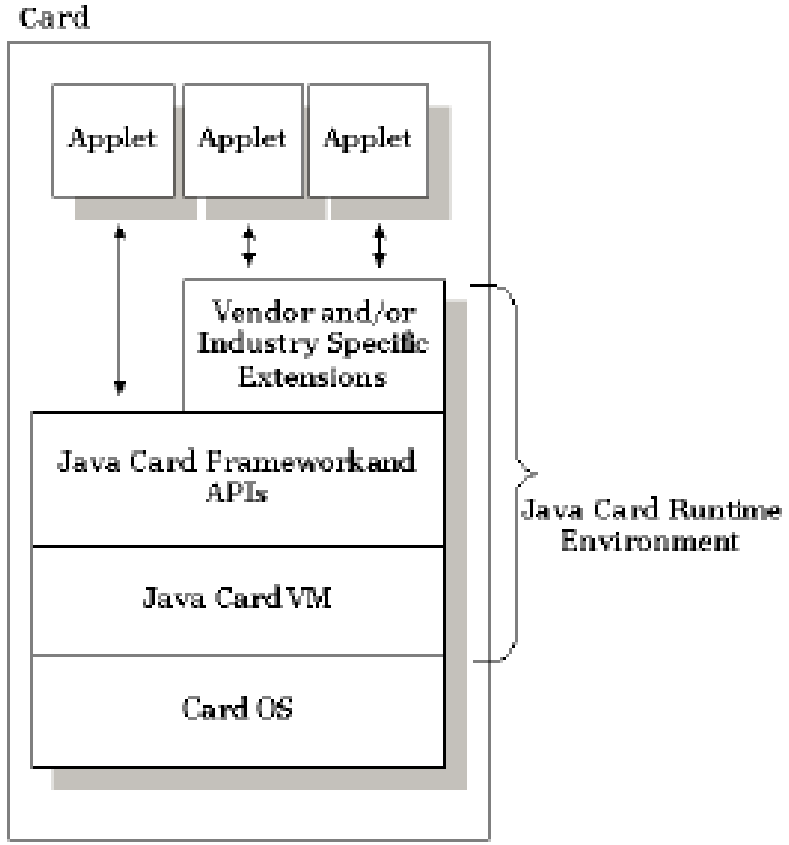
Application Protocol Data Unit (APDU)

Application Protocol Data Unit (APDU)



JavaCard Runtime Environment- JCRE

- Life time
  - initialized at card initialization time (only once)
  - after each reset, JCRE enters “receive-process-reply” loop
  - applets and persistent data are preserved over resets
- Responsible for
  - card resource management
  - network communication
  - applet execution
  - system and applet security
- Defines the JavaCard API



JavaCard Virtual machine - JCVM

- JCVM
  - Interprets Java „byte code“
  - Is a subset of the Java desktop Virtual machine
- Supported Java features JavaCard 2.2
  - small primitive data types: boolean, byte, short
  - one-dimensional arrays
  - packages, classes, interfaces, and exceptions
  - object-oriented features: inheritance, virtual methods, overloading and dynamic object creation
  - access scope, and binding rules
  - garbage collection
  - optional: int

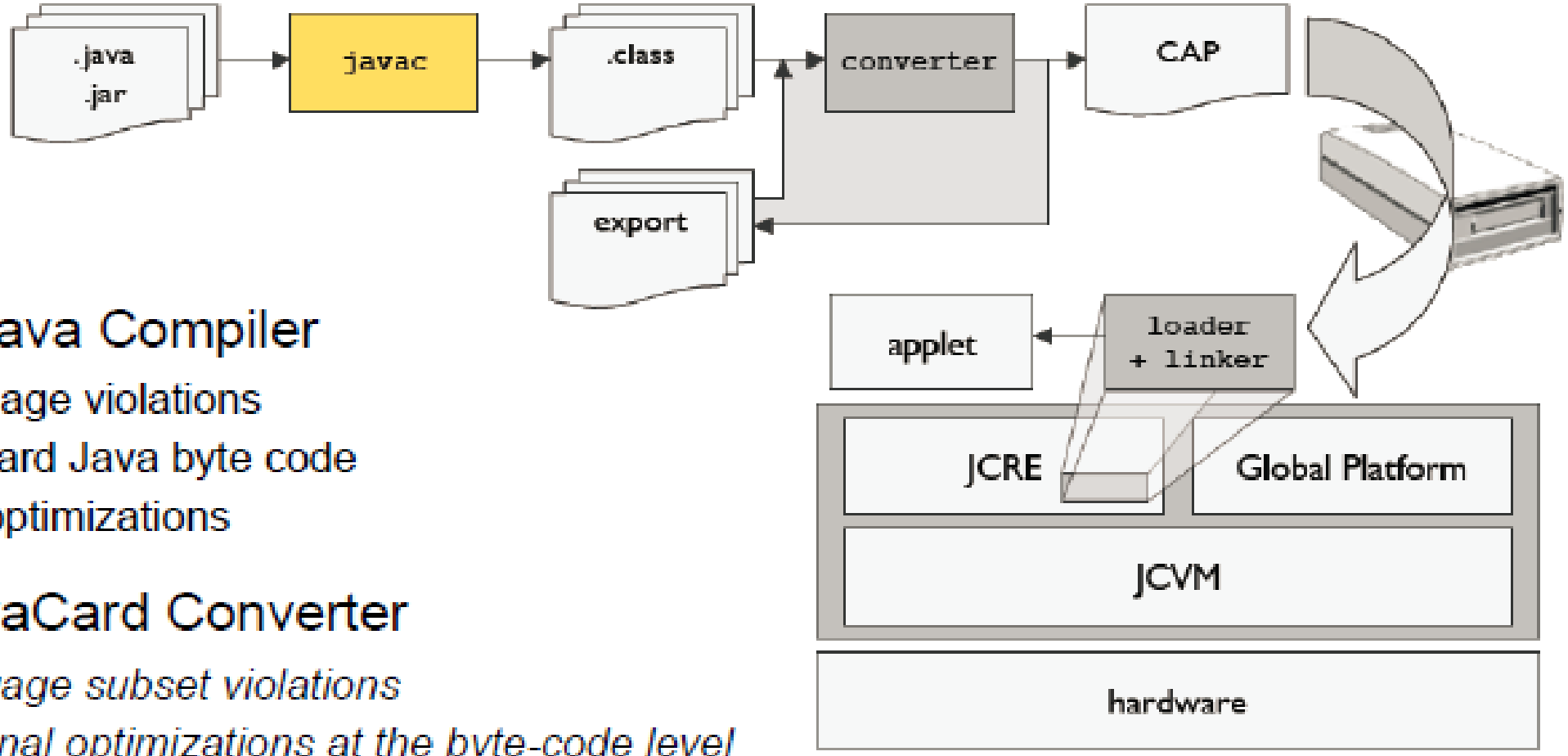
JavaCard Virtual machine - JCVM

- Unsupported Java features JavaCard 2.2
  - characters and strings
  - large primitive data types: long, double, float
  - finalization (and garbage collection prior to JC 2.2)
  - multi-dimensional arrays
  - dynamic class loading
  - security manager
  - object serialization and cloning
  - threads

Java Card Cryptographic Support

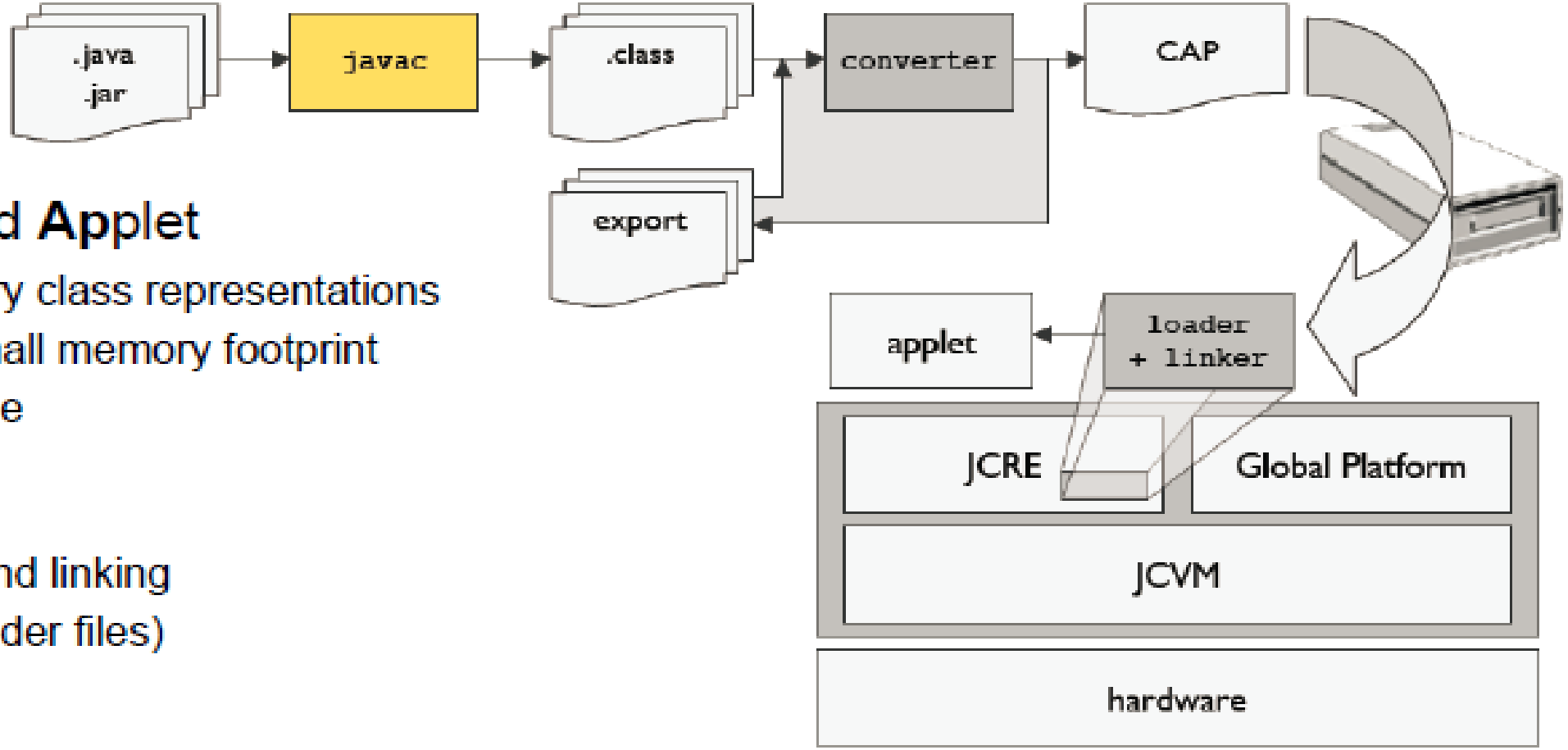
- javacardx.crypto.Cipher
- javacard.crypto.Signature
- javacard.security.MessageDigest
- javacard.security.RandomData
- javacard.security.KeyPair
  - DES, RSA, DSA, Elliptic Curves,
- javacard.security.KeyAgreement
  - Diffie Hellman
- javacard.security.Checksum;

Secure Element Development Process



1. Write Applet
2. Compile it with Java Compiler
   - checks for language violations
   - generates standard Java byte code
   - performs basic optimizations
3. Convert with JavaCard Converter
   - *checks for language subset violations*
   - *performs additional optimizations at the byte-code level*
   - allocates storage and creates VM data structures to represent classes

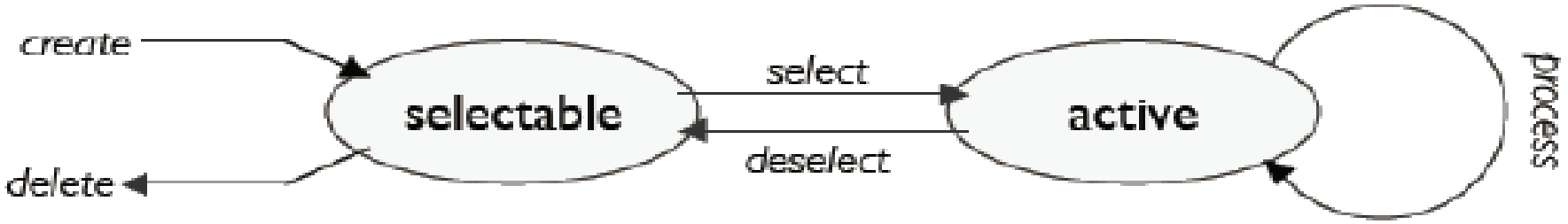
Secure Element Development Process



4. CAP – **C**onverted **A**pplet
   - executable binary class representations
   - optimized for small memory footprint
   - only one package
5. Export
   - for verification and linking
   - (similar to C header files)
6. Loader/Linker
   - assembles a CAP file into an executable applet or a linkable shared library
7. JCVM
   - Stack machine
   - Executes Java byte-code

JavaCard Applet

- Definition
  - an Applet extends the **javacard.framework.Applet** class
  - an Applet is uniquely identified by an AID
  - any number of applets may be installed
  - only one applet is running at a time
- Applet life cycle
  - applet's life starts when it is registered with the JCRE
  - must be explicitly selected by the host
  - purely reactive behaviour



JavaCard Applet Class

```
public abstract class Applet {
    public static void install(byte[] bArray, short bOffset, byte bLength);
    protected final void register();
    protected final void register(byte bArray, short bOffset, byte bLength);
    public boolean select();
    public void deselect();
    protected final boolean selectingApplet();
    public abstract void process(APDU apdu);
    ...
};
```

- Creates an ins
- Should perfor
- Installation is
- After successf

```
public class myApplet extends Applet {
    public static void install(byte[] bArray, short bOffset, byte bLength) {
        (new myApplet()).register(bArray,(short)(bOffset+1),bArray[bOffset]);
    }
    protected myApplet() { // constructor
        ...
    }
};
```

JavaCard Applet Class

```
public abstract class Applet {
    public static void install(byte[] bArray, short bOffset, byte bLength);
    protected final void register();
    protected final void register(byte bArray, short bOffset, byte bLength);
    public boolean select();
    public void deselect();
    protected final boolean selectingApplet();
    public abstract void process(APDU apdu);
    ...
};
```

- Registers the new applet instance with the JCRE
- Uses the AID specified in the CAP file (only one applet instance possible), or
- The AID passed in bArray (multiple instances possible)

JavaCard Applet Class

```
public abstract class Applet {
    public static void install(byte[] bArray, short bOffset, byte bLength);
    protected final void register();
    protected final void register(byte bArray, short bOffset, byte bLength);
    public boolean select();
    public void deselect();
    protected final boolean selectingApplet();
    public abstract void process(APDU apdu);
    ...
};
```

- Called by the JCRE to inform the applet that it has been selected
- Default applet is selected automatically on card reset
- Returns “false” if the applet cannot be selected (e.g. remaining PIN count is 0) otherwise “true”

JavaCard Applet Class

```
public abstract class Applet {
    public static void install(byte[] bArray, short bOffset, byte bLength);
    protected final void register();
    protected final void register(byte bArray, short bOffset, byte bLength);
    public boolean select();
    public void deselect();
    protected final boolean selectingApplet();
    public abstract void process(APDU apdu);
    ...
};
```

- Called by the JCRE to inform the applet that another (or the same) applet will be selected
- Needed to cleanup before the JCRE gives control to the newly selected applet (e.g. PIN is no longer validated)

JavaCard Applet Class

```
public abstract class Applet {
    public static void install(byte[] bArray, short bOffset, byte bLength);
    protected final void register();
    protected final void register(byte bArray, short bOffset, byte bLength);
    public boolean select();
    public void deselect();
    protected final boolean selectingApplet();
    public abstract void process(APDU apdu);
    ...
};
```

```
public class myApplet extends Applet {
    public void process(APDU apdu) {
        if (selectingApplet()) {
            ... // the applet was selected
            return;
        }
        ... // process APDU
    }
};
```

- called by the J
- upon normal r
  the APDU resp
- **selectingApplet**: used by the process method to distinguish between applet selects from other SELECT APDU commands

JavaCard Applet: Processing Requests

```
public void process(APDU apdu) throws ISOException
{
      byte[] buffer = apdu.getBuffer();
      // .. process the incoming data and reply
      if ( buffer[ISO7816.OFFSET_CLA] == (byte)0 )
      {
          switch ( buffer[ISO7816.OFFSET_INS] )
          {
              case ISO.INS_SELECT:
                  ... // send response data to select command
                  short Le = apdu.setOutgoing();
                  // assume data containing response bytes in replyData[] array.
                  if ( Le < ..)
                      ISOException.throwIt( ISO7816.SW_WRONG_LENGTH);

                  apdu.setOutgoingLength( (short)replyData.length );
                  apdu.sendBytes(replyData, (short) 0, (short)replyData.length);
                  break;

              case ...
```

Ultra Secure Elements: desired specs

1- Powerful compute power:

- ❑ 32-64 bit RISC processor to perform advanced encryption
- ❑ Embedded Secure Operating System (Javacard,…)

2- Secure Memory – 100KB to 1MB:

- ❑ Store and manage multiple secret cryptographic keys
- ❑ Store user data base
- ❑ Cache memory to store and run the OS

3- Contain Physically Unclonable Functions (PUF)

- ❑ Electronic "fingerprint

4- Contain Random Number Generator (RNG)

- ❑ True RNG are based on physical randomness

5- Resist side channel attacks (DPA, SPA, EMI,…)

- ❑ Incorporate confusion techniques

6- Easy to deploy: Fast "personalization" and cost effective

Thank You!!!

Q & A

bertrand.cambou@nau.edu